Analysis on Exposed IoT Assets in China (March 2017)

■ Document No.:	■ Confidentiality:
■ Issue:	■ Date:

■ **Change History**

Date	Issue	Description	Prepared/Modified By

Contents

Figures

Tables

1 Overview

With the maturity of sensing, computing, and communication technologies, the Internet of Things (IoT) will be more and more widely used in various industries. Gartner, a market research agency, predicts that endpoints of the IoT will grow at a 33% CAGR from 2015 through 2020, reaching an installed base of 20.4 billion units, with almost two-thirds of them consumer applications. Spending on networked consumer and business endpoints will displace non-networked, growing at a 20% CAGR to $2.9 trillion. In 2016, IoT was written into the Thirteenth Five-Year Plan, which pointed out that efforts should be made to push the development of cloud computing and IoT, promote the planning layout of IoT-aware facilities, and develop open-loop IoT application. This suggests that the government attaches great importance to various types of IoT infrastructure and applications strategically. Meanwhile, many IoT devices and applications are facing severe security challenges. On September 20, 2016, the famous security journalist, Brian Krebs's website, KrebsOnSecurity.com, was attacked by a large-scale distributed denial-of-service (DDoS) attack, whose traffic peaked at 665 Gbps. Brian Krebs speculated that this attack was launched by means of the Mirai botnet. On the same day, France-based hosting service provider OVH became a victim of the record-breaking DDoS attacks that reached 1 Tbps, with peak traffic of 1.5 Tbps. On October 21, 2016, Dyn, a US-based DNS provider, received a global DDoS attack, whose attack source was confirmed to be the Miari botnet. This attack finally led to a massive network outage in the east coast of the United States. On November 28, 2016, a new Mirai variant disrupted Deutsche Telekom services. The reason why Mirai botnets are widely spread is that IoT devices exposed on the Internet are prone to security issues, such as weak passwords.

It is important to note that a majority of Mirai-infected IoT devices are directly exposed on the Internet. Therefore, it is noteworthy to research on exposed IoT assets. A feasible research methodology is to locate related IoT devices by using cyberspace search engines.

Unlike Internet search engines (such as Google and Baidu), cyberspace search engines (such as NTI[1], Shodan[2], and ZoomEye[3]) focus on IP addresses, corresponding devices, and services running on these devices. NSFOCUS Threat Intelligence (NTI) is a threat intelligence platform of NSFOCUS. According to detection results, security researchers can find vulnerabilities and quickly grasp the global distribution of such vulnerabilities.

In 2016, Trend Micro released a research report[9] based on Shodan data, which analyzed the exposed six key sectors (the government, emergence services, healthcare, utilities, finance, and education) on the Internet in America. At the 2017 RSA Security Conference, a researcher from Trend Micro delivered a keynote speech on the report content. In the IoT-related analysis, the report mainly focuses on the industrial control system. Though video surveillance devices and routers are mentioned, they are not the focal point and only mentioned as products detected in an industry.

In the context that IoT-related security issues are attracting more and more attention, it is necessary to analyze and identify IoT assets exposed on the Internet. Related data can be

obtained for analyzing IoT security situation, solutions, and technically assessing vulnerabilities and risks.

In terms of the technical roadmap, considering the great differences between domestic and international IoT systems and products, this paper mainly analyzes IoT assets in China and describes their exposure, such as their distribution among cities and the distribution of ports on them, to illustrate what services are accessible on the Internet and potential security problems, with the purpose of raising the public awareness of IoT threat defense.

In chapters 2 and 3, the analysis is made respectively from the perspectives of IoT devices and IoT operating systems (OSs). Chapter 2 describes IoT devices exposed on the Internet and their distribution. Chapter 3 describes common IoT (OSs), providing readers with some knowledge of the OSs exposed on the Internet.

It is worth noting that, when an IoT device is exposed on the Internet, this does not necessarily mean that this device is vulnerable, but suggests that it is at risk of being attacked and exploited. For example, for a device that allows users to log in by typing a correct user name and password, if the user adopts a complex password, this device is not prone to a weak password vulnerability. However, once exposed on the Internet, the device will have a larger attacker surface. In an unexpected security event (such as heartbleed), the vulnerability in its Internet-exposed services will be found and exploited.

1.1 Research Methodology

This analysis is conducted based on NTI, ZoomEye, and Shodan data. There are mainly two data sources: One is information about the devices identified by search engines. If believing such information correct, we will directly use such information, for example, using "service:DAHUA-DVR" as the keyword on NTI to search for information about Dahua DVRs. The other data source is the search results of vendor names and models[①]. We will observe the search results and then adjust search keywords until satisfactory results appear. Here, take routers as an example. We first search for most models of mainstream home routers. For Hikvision products, we find that the banner[②] information of some services of their cameras contains "Server: Hikvision-Webs". Therefore, we can use this character string as the keyword to search for Hikvison cameras.

Statement:

All data in this report comes from such public cyberspace search engines as NTI, Shodan, and ZoomEye.

1.2 Key Findings

By analyzing common IoT devices and OSs, we find as follows:

① We obtained model information from the respective official websites.

② Banner information refers to the return information received by search engines in the process of detecting IP addresses and ports. Take an HTTP message as an example. The received result contains HTTP headers and body. "Server: Hikvision-Webs" resides in the HTTP header section.

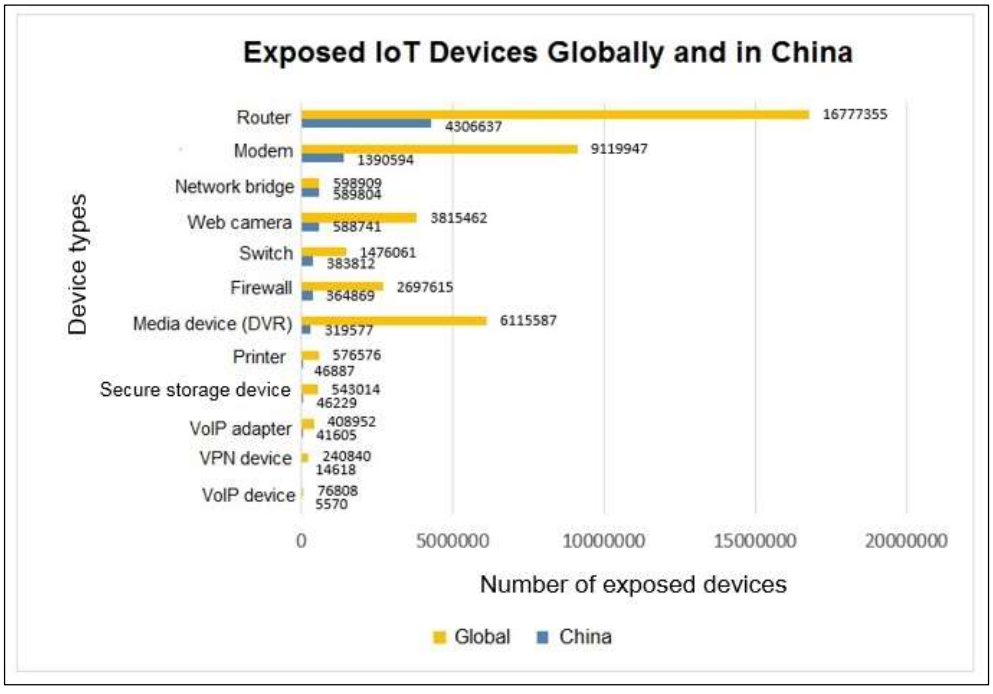
- Hikvision and Dahua have the most exposed network surveillance devices. Coastal provinces in the southeastern part of China witness the most exposed devices.
- Most routers exposed to China's Internet are of domestic brands. The ports of these exposed routers mainly adopt UPnP and FTP protocols. The Sales of routers from Internet vendors are booming, with few exposed on the Internet.
- Thousands of routers in China are infected with malware Linux.Wifatch. The security situation of routers is not optimistic
- Hong Kong and Taiwan have the most exposed network printers, accounting for over 95% of the printers.
- The reason why most devices carrying an OS are probed is that they are deployed on the Internet with no default settings changed. For example, among the 7924 ports opened for the HTTP service on devices running DD-WRT, 22.6% are exposed because their titles contain "DD-WRT (build xxxxx="infopage">". 98.6% devices running uClinux contain such banner information as "Server: uClinux/2.6.28.10 UPnP/1.0 MiniUPnPd/1.3".
- For a device that runs DD-WRT or uClinux and functions as a router, performing network address translation (NAT) makes it possible for its IP address to embody combined properties of multiple devices.

2 Exposure of Common IoT Devices in China

2.1 Introduction

Smart devices are becoming an integral part of people's daily lives. Though IoT devices are very convenient, potential security issues should not be underestimated. Through data collection and analysis, we have learned that a dozen or so IoT devices are severely exposed, which are presented in Figure 2-1 in the descending order of the number of exposed devices. As shown in Figure 2-1, Internet-connected devices are most exposed. In China, routers and top the list, with a total number of more than 5 million.

Figure 2-1 Exposed IoT devices globally and in China



Of course, IoT device are far more than those presented in the figure. On the one hand, some lesser-known devices (such as access control device, temperature monitoring system, and vehicle dispatching system) and the devices used in special industries are not listed. If necessary, we will complement or update device information in subsequent reports. On the

other hand, many IoT devices connect to LANs and communicate with IoT-based applications via NAT. Hidden among gateway devices, such devices will not be exposed on the Internet.

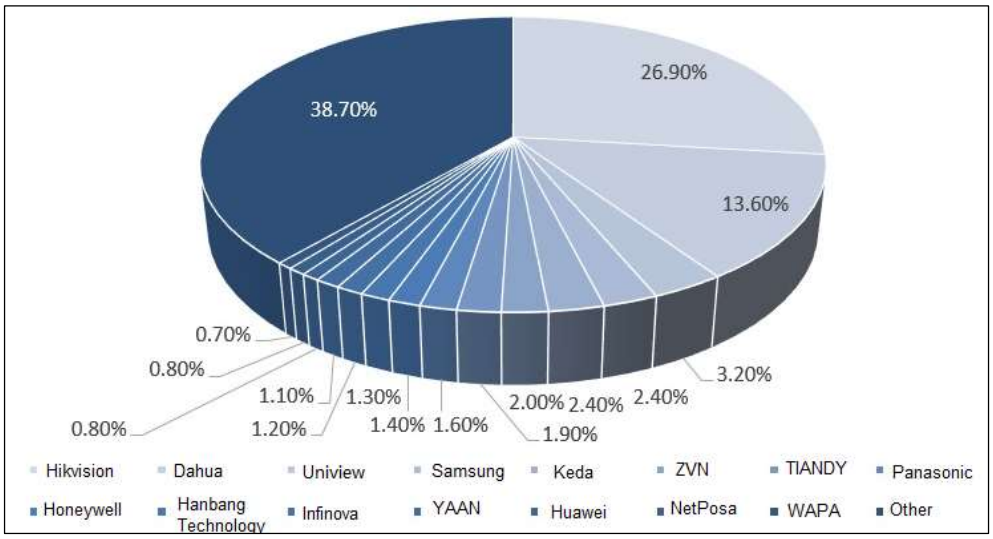
2.2 Video Surveillance Devices

As very important IoT devices, video surveillance devices have been involved in many international IoT security events in the past several years. Therefore, this section provides statistics on and analyzes exposed video surveillance devices in China.

2.2.1 Overall Picture

According to the *World Market for CCTV and Video Surveillance Equipment (2014)* released by IHS, Hikvision, Dahua, Axis Communications, Panasonic, Samsung Techwin, Bosch Security Systems, Pelco, Honeywell, Avigilon, Tyco, Sony, Uniview, Aventura, UTC, and Infinova were the top 15 vendors enjoying the biggest market share. Hikvision was number one, followed by Dahua. However, the gap between the two was huge[19]. Figure 2-2 shows the market shares of video surveillance devices in China in 2013 released by HIS.

Figure 2-2 Market shares of video surveillance devices in China in 2013



By investigating the exposure of the preceding video surveillance devices and that of devices from other vendors, we find as follows:

Viewpoint 1: Hikvision and Dahua have the most exposed devices.

Up to today, the products from a dozen or so network surveillance device (network hard disk camera, web camera, and video server) vendors are suffering a varying degrees of exposure. Hikvision and Dahua have the most exposed devices.

Figure 2-3 Exposed network surveillance devices in China

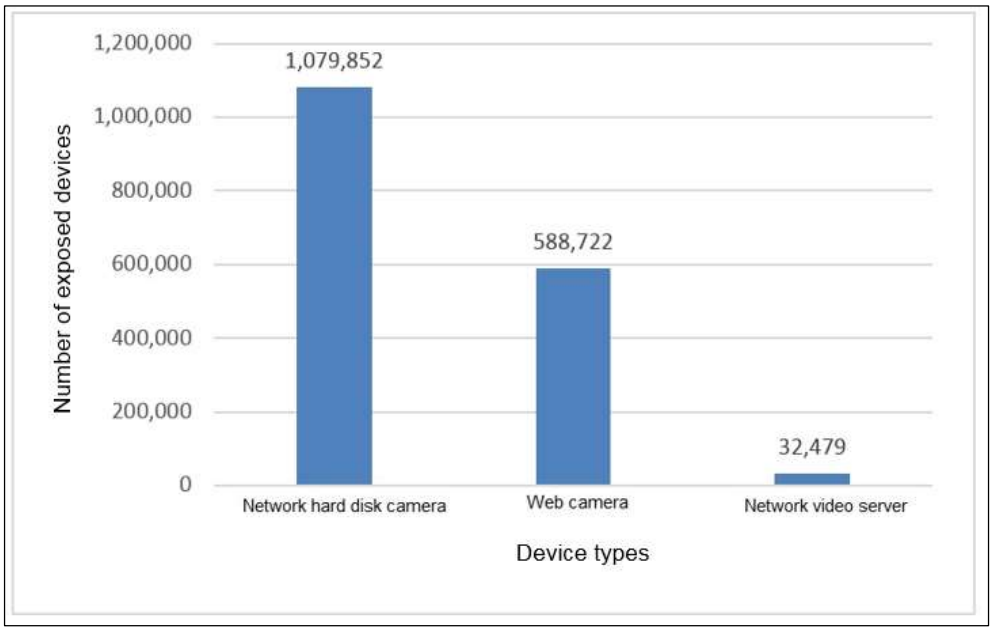
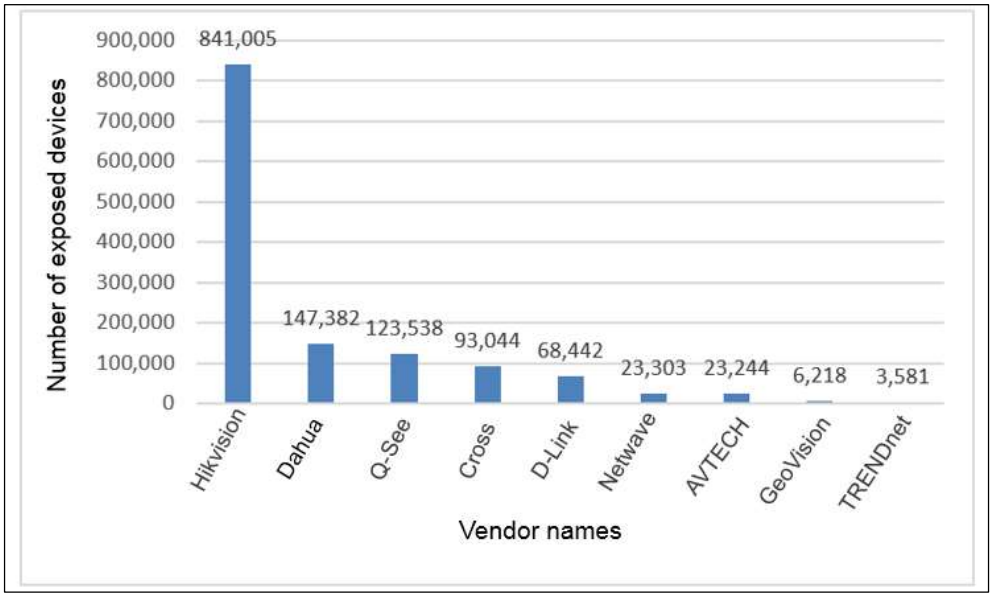


Figure 2-4 Distribution of vendors with exposed devices



As shown in Figure 2-3 and Figure 2-4, more than one million surveillance devices are exposed in China, mostly network hard disk cameras. However, the number of exposed devices from Hikvision and Dahua reaches nearly one million.

2.2.2 Analysis of Specific Vendors

As shown in Figure 2.4, Dahua and Hikvision have the most exposed network surveillance devices. This section takes them as the main analysis object and conducts the analysis from the perspectives of open port and geographical location.

Open Ports

Viewpoint 2: The ports exposed on network surveillance devices are mostly the default ones.

Table 2-1 lists the ports frequently appearing, common ports, and corresponding protocols on exposed devices. According to our investigation, default ports vary with surveillance device vendors. For example, the default port for the video data service of Dahua surveillance devices is 37777 and that for the data service of Hikvision devices is 8000. Likewise, attackers can also find these default ports by referring to related materials and then scan to locate devices. Therefore, we recommend that the default port of each service should be changed, thereby reducing the risk of being detected by the attacker's broad-spectrum scanning.

Figure 2-5 Exposed ports of network video surveillance devices

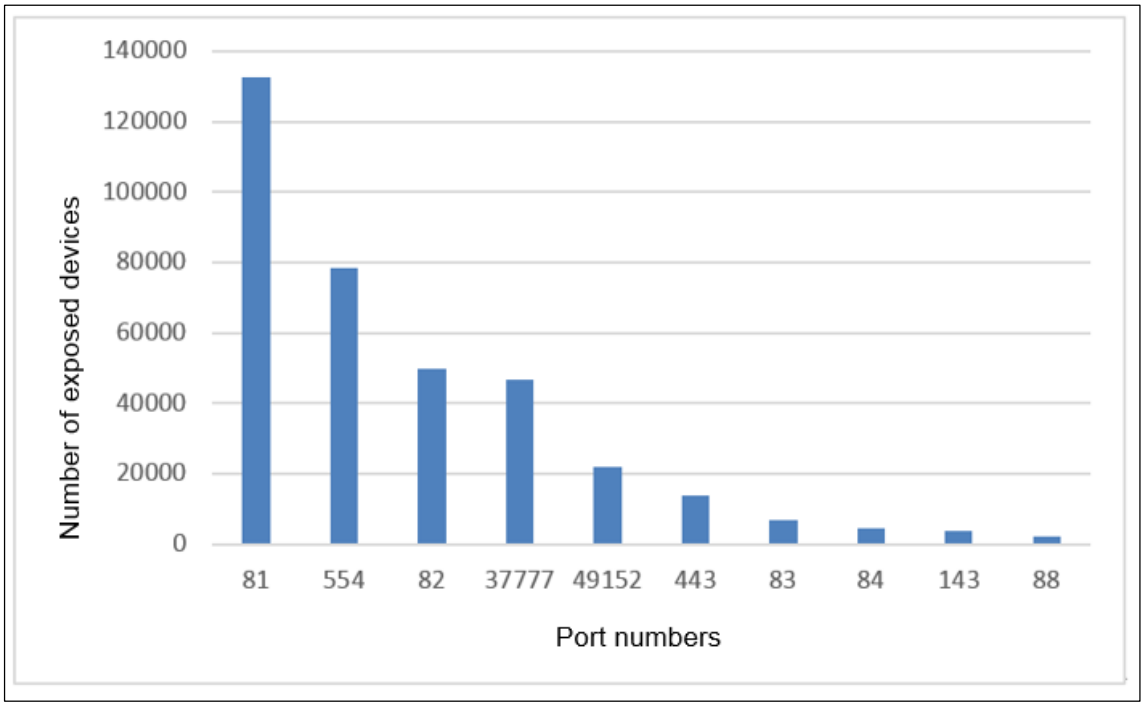


Table 2-1 Mappings between ports and protocols of video surveillance devices

Port	**80**	**554**	**443**	**49152**	**8080**
Protocol	HTTP	RSTP	HTTPS	UPnP	HTTP

2.3 Home Routers

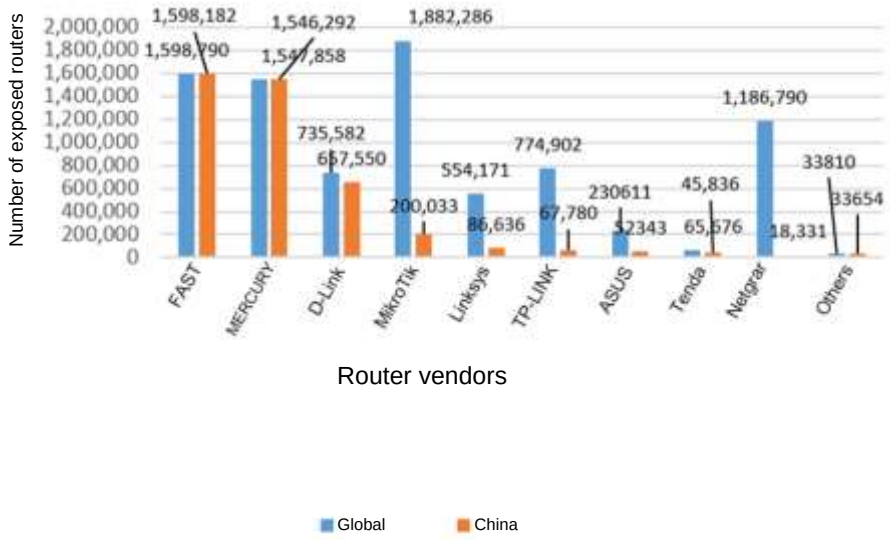
Home routers differ widely from enterprise routers in application scenarios and performance requirements. We have searched for home routers of popular brands such as FAST, MERCURY, TP-LINK, and Xiaomi. This section describes the exposure of these home routers[③].

2.3.1 Overall Picture

Viewpoint 3: Most routers exposed on China's Internet are of domestic brands.

As shown in Figure 2-6, routers from domestic vendors such as FAST, MERCURY, D-Link, and Tenda are largely for domestic use. Also, TP-LINK and ASUS (based in Taiwan) are also Chinese vendors.

Figure 2-6 Exposure of routers from major domestic vendors



Viewpoint 4: Routers from Internet vendors are booming, with few exposed on the Internet.

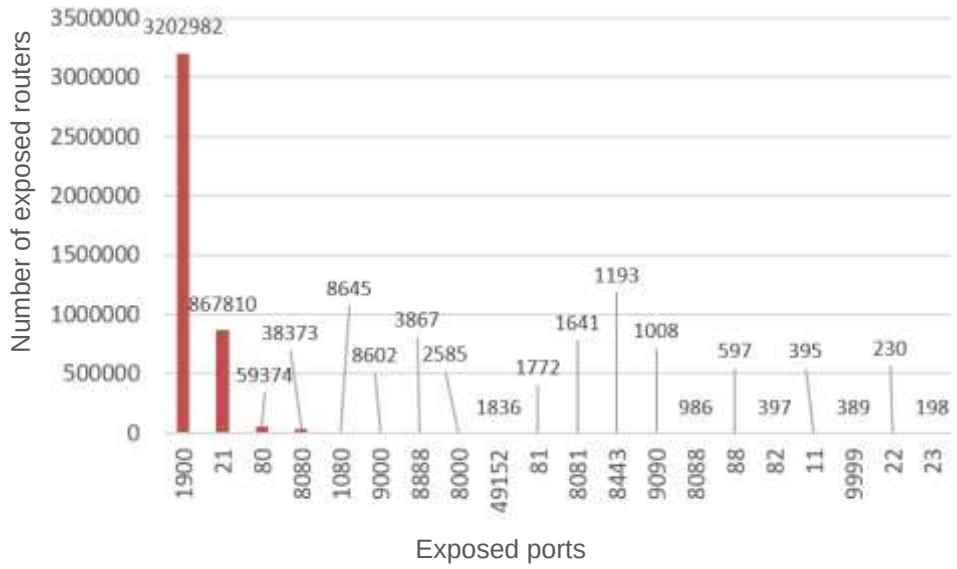
[③]As many a router models of various vendors are involved, data in this chapter may cover some enterprise routers.

Sales for routers from Internet vendors are soaring. In January 2017, over 10,000,000[17] Xiaomi routers were sold. According to iiMedia Research[18], in the first half of 2016, Qihoo 360 security routers topped the ranking of smart routers with a market share of 51.5%. Figure 2-6 shows that most exposed routers are from traditional vendors, accompanied by a small number of routers of such emerging brands as Xiaomi④, 360⑤, and HiWiFi⑥.

Viewpoint 5: Home routers use a wide range of ports, mostly ports 1900, 21, 80, and 8080.

From the port distribution, we see that home routers use a total of 39 ports. Figure 2-7 shows top 20 exposed ports. The remaining 19 ports are exposed 364 times in total. You can see that though so many ports are used, only some are exposed frequently.

Figure 2-7 Distribution of home routers by port



Viewpoint 6: Exposed ports of routers mainly adopt Universal Plug and Play (UPnP) and FTP.

④Few Xiaomi routers are found (when we search for "Xiaomi Mini" and "MiWiFi"). Those routers are assigned as the Other category, together with Qihoo 360 security routers and HiWiFi routers.

⑤Qihoo 360 and Netcore together started a joint venture to produce security routers. After we search for "netcore" on NTI, we find routers of this vendor. However, models of those routers suggest that they are not security routers launched by the joint venture.

⑥After we search for "hiwifi" on NTI, HiWiFi routers are found.

Table 2-2 shows the most frequently used ports and common ports (such as ports 22 and 23) as well as protocols used by those ports. For routers exposed on the Internet, the most widely used protocol is UPnP which is followed by FTP.

Table 2-2 Mappings between frequently used ports and their adopted protocols

Port	1900	21	80/8080	22	23
Protocol	UPnP	FTP	HTTP	SSH	Telnet

UPnP allows applications (or host devices) to automatically discover frontend NAT devices and request such devices to open corresponding ports. After enabling UPnP, applications (or host devices) at both ends of NAT can exchange information independently to achieve seamless connections between devices. Users may enable UPnP when using applications for multiplayer games, point-to-point connections, real-time communication (such as Internet calls and conference calls) or remote assistance.

As UPnP is enabled on many routers by default, it is the greatest blame for the exposure of routers.

More than 800,000 devices have port 21 exposed. TP-LINK's official website[8] shows that dual-band wireless router series products can serve as FTP servers after they are connected to mobile storage devices. Users can share images, movies, and music via FTP.

Some routers (including MERCURY routers) support remote management via the Internet. This may cause some HTTP protocols to be spotted. However, once routers are properly configured, users usually will not easily change such configurations and rarely require remote router management. Therefore, you are advised to disable the remote management function.

Finally, we found that HTTP data transmitted over ports 80 and 8080 faces the hijacking risk due to the lack of encryption.

2.3.2 Analysis of Specific Vendors

During analysis, we found that some vendors have a unique distribution of exposed devices. Here, we focus on FAST, MERCURY, and TP-LINK.

2.3.2.1 FAST and MERCURY

Viewpoint 7: FAST and MERCURY share very similar port distribution and banner for exposed devices.

During search, we found that routers from FAST and MERCURY have two similarities:

- Port 1900 is mainly used.
- Port 1900 corresponds to similar contents.

Figure 2-8 and Figure 2-9 respectively present the port distribution of routers from the two vendors. We can see that these routers mainly use port 1900.

Figure 2-8 Port distribution of routers from FAST

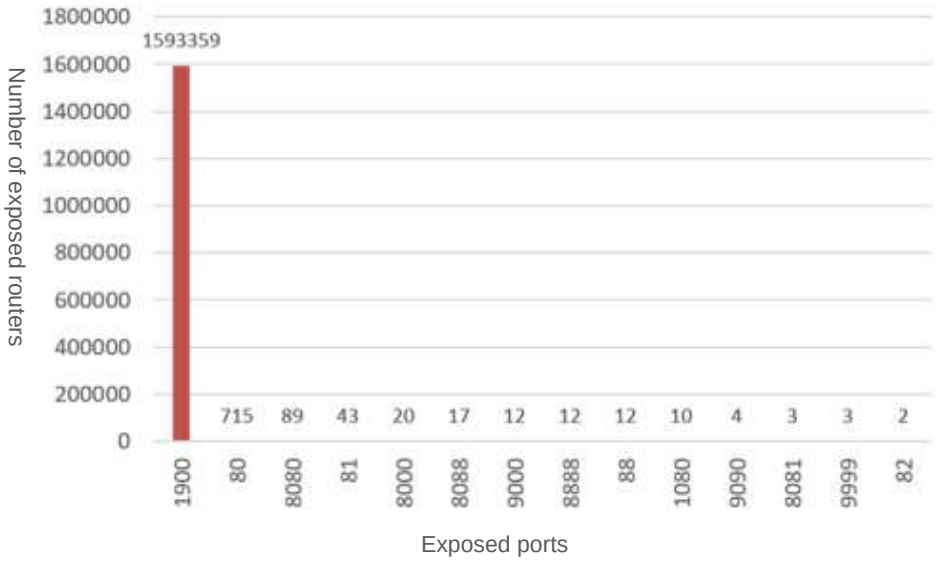


Figure 2-9 Port distribution of routers from MERCURY

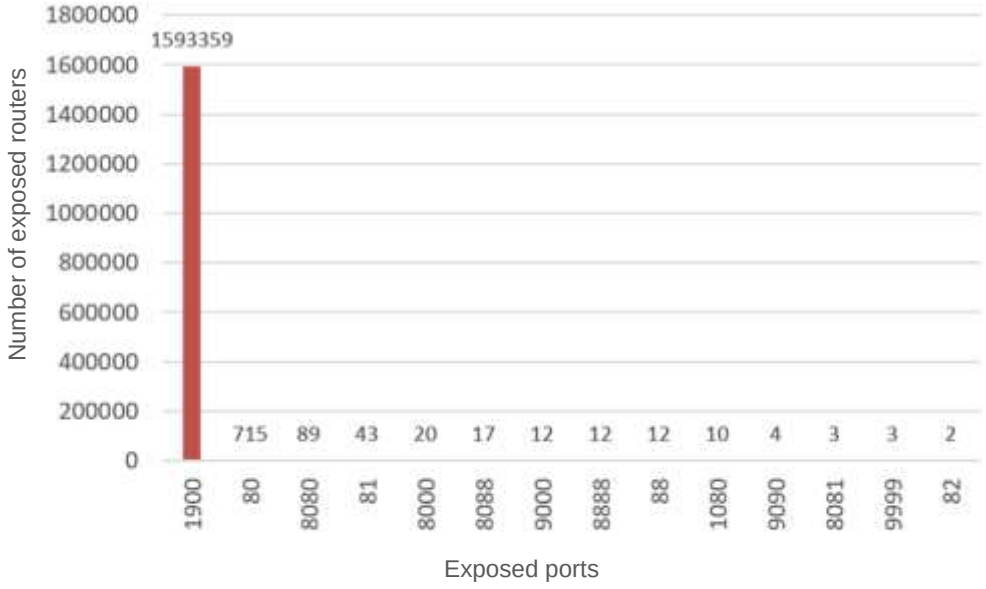


Figure 2-10 and Figure 2-11 respectively show port 1900 and banner information of FW313R (from FAST) and MW313R (from MERCURY). We can see that both routers have the same banner information except the device model.

Note that the banner information contains the device model, but without vendor information. We find the vendors by searching for the two models respectively in a search engine.

Figure 2-10 Banner of FW313R

Port	Service	Banner
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

Figure 2-11 Banner of MW313R

Port	Service	Banner
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

Viewpoint 8: Three FAST routers and four MERCURY routers respectively account for more than 99% of the total exposed routers of the vendor.

Though FAST and MERCURY both provide many router models, the majority of exposed routers are of several models. For FAST[7], FWR310, FW300R, and FW313R routers make up 99.76% of the total exposed devices. For MERCURY, MW310R, MW300R, MW305R, and MW313R routers comprise 99.69% of all exposed routers.

Figure 2-12 Number of FAST and MERCURY routers of major exposed models

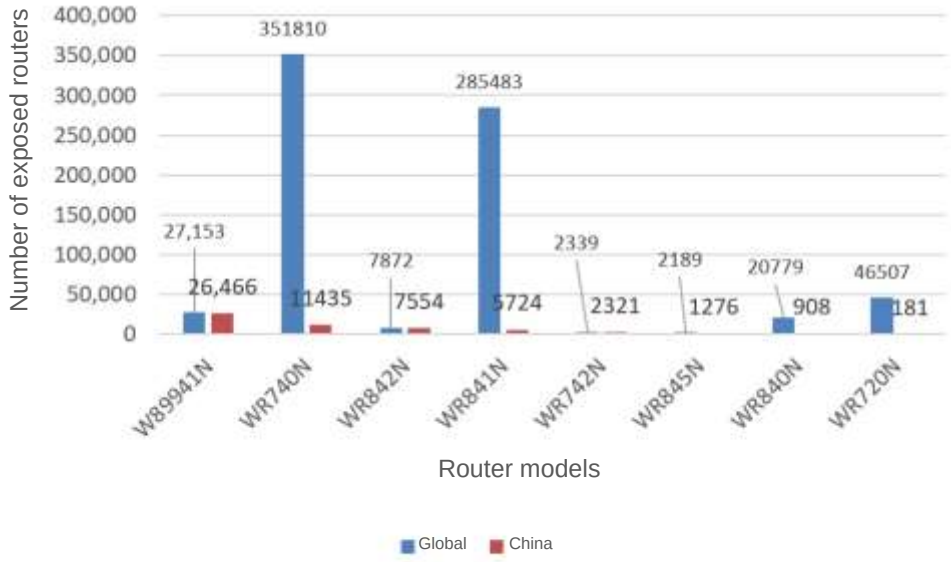
[7]We obtained all device models on sale of the two vendors on their official websites.

2.3.2.2 TP-LINK

Viewpoint 9: 8.7% of TP-LINK routers are located domestically, with eight models making up 82% of the domestic total.

Also, there are many TP-LINK router models, but most exposed routers are of a few models. Unlike FAST and MERCURY routers that are mostly sold on the home market, only 8.7% of TP-LINK routers are deployed domestically.

Figure 2-13 Number of TP-LINK routers of major exposed models



Viewpoint 10 Exposed TP-LINK router models adopt different protocols.

Table 2-3 Mappings between TP-LINK router models and their adopted protocols

Model	W89941N	WR740N	WR842N	WR841N	WR742N
Protocol	UPnP	Mainly HTTP	Mainly HTTP	Mainly HTTP	Mainly HTTP supplemented by UPnP

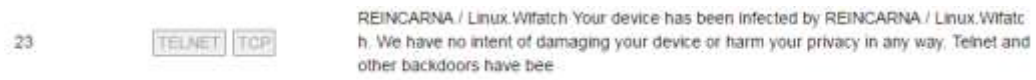
Obviously, different router models have different ports exposed. To show the difference, we list protocols adopted by exposed ports of top five router models.

2.3.3 Other Findings

Viewpoint 11: Thousands of devices are infected with Linux.Wifatch in China.

During router information analysis, we accidentally found that port 23 on some routers returns the following information:

Figure 2-14 Banner of Linux.Wifatch



Linux.Wifatch is a kind of malware that appeared in November 2014. With the aid of remote login (via Telnet) and other protocols, it infects devices that use weak passwords or default passwords. Once the infection succeeds, this malware disables Telnet and presents the banner information shown in Figure 2-14.

In October 2015, a researcher named Mario Ƀarano from Symantec gave a detailed introduction to this malware, revealing that it has infected thousands of routers, web cameras, and other devices. At that time, domestic security media such as FreeBuf[4] and AQNIU also published articles to report this malware.

Interestingly, though Linux.Wifatch infects Internet of Things (IoT) devices, it keeps out other malware, instead of performing malicious behaviors. It seems that this malware "protects" infected devices. For details about this open-source malware, visit https://gitlab.com/rav7teif/linux.wifatch.

According to data on NTI, 93,480 devices are currently tainted with this malware in the world, including 14,347 devices in China.

Figure 2-15 Search results of Linux.Wifatch on NTI

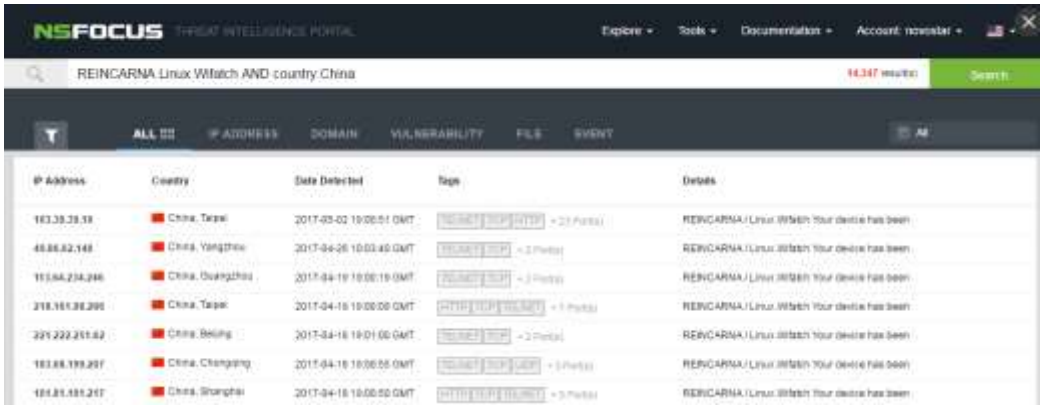
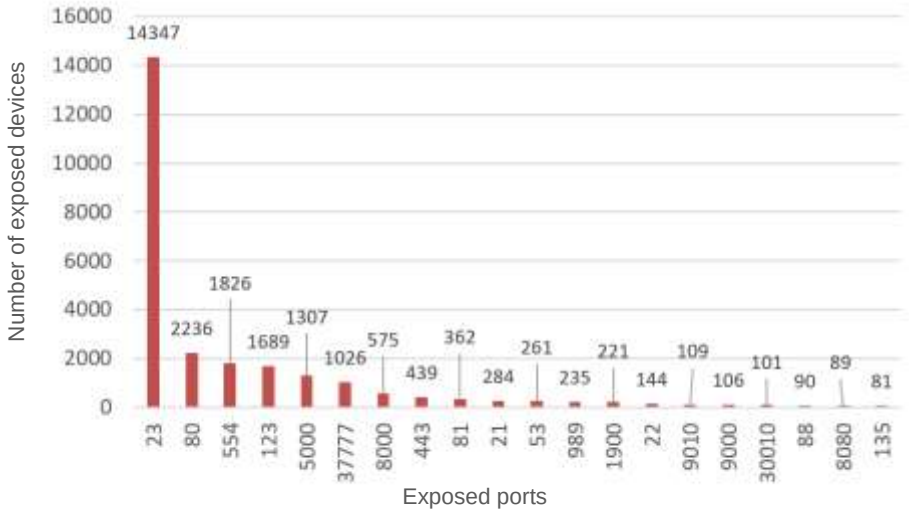


Figure 2-16 shows device statistics by exposed port. Multiple devices tainted with Linux.Wifatch only have port 23 or a few other ports exposed. Merely judging from exposed ports, it is hard to determine the infected devices, most of which are possibly routers. Besides, video surveillance devices usually have ports 554 and 37,777 exposed.

Figure 2-16 Exposed ports of devices tainted with Linux.Wifatch



Restoring factory defaults of routers and restarting them can remove this malware. However, if you do not upgrade the firmware or change weak passwords, routers may be infected against.

2.4 Printers

It is widely known that printers play an important role in business scenarios. In the Internet Plus era, enterprises have a growing demand for mobile printers, which propels the emergence of more and more so-called "smart" printers. Major functional difference between common printers and smart printers lies in the support for direct Wi-Fi connections, NFC printing, cloud printing, and other mobile printing functions[16]. Though smart printers bring convenience to us, whether security issues exist in these printers is worthy of consideration.

It is worth to mention[7] security events occurring in Taiwan in March 2017. At that time, hackers attacked printers in many schools in Taiwan, threatening to paralyze their networks if they refuse to pay the requested ransom. Actually, most network printers use external IP addresses and some school printers and IoT devices use default passwords. Therefore, those devices are directly exposed to attackers, giving rise to more and more similar security events.

Viewpoint 12: The sum of exposed Hewlett-Packard (HP) and Epson printers account for over 50% of the exposed total.

As printers serve as network terminal devices, their related security issues should be taken seriously by customers and vendors. Figure 2-17 shows the distribution of printer market shares in 2015, according to the *2015-2020 Chinese Laser Printer Industry Market Outlook and Investment Strategy Planning Analysis Report*[14] released by the forwarding-looking industry institute. We have searched for exposed printers of different brands and presented the exposed quantity by brand as shown in Figure 2-18. Different brands of printers have different numbers of devices exposed. Currently, HP, Epson, and Fuji Xerox are top three exposed brands, contributing to more than 75% of the exposed total.

Figure 2-17 Distribution of printer market shares in 2015

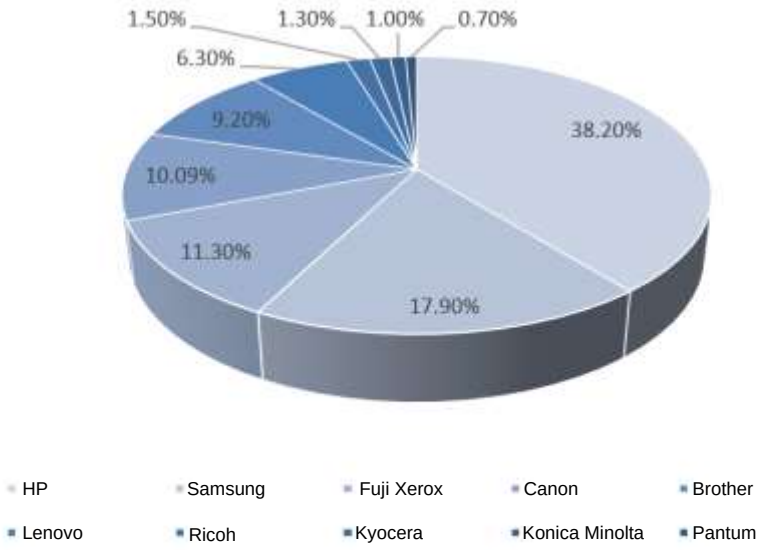
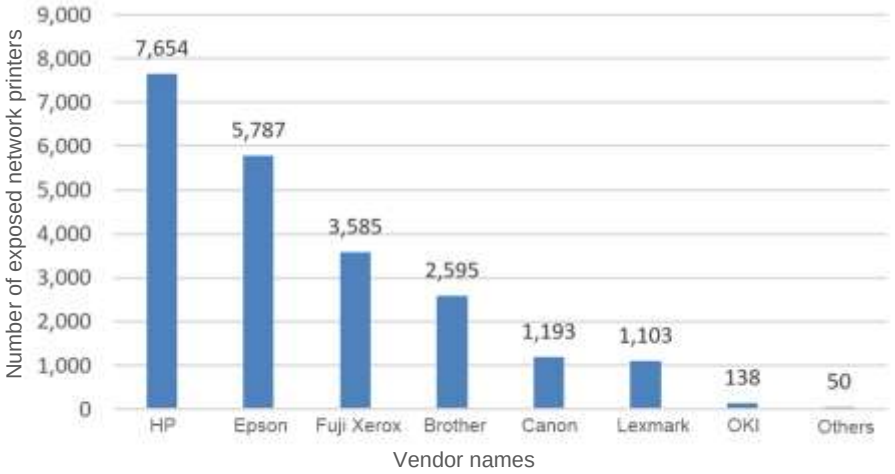


Figure 2-18 Distribution of exposed network printers by brand



Viewpoint 13: Exposed network printers most distribute in Hong Kong and Taiwan, accounting for over 95% of the total exposed.

As shown in Figure 2-19, exposed network printers mainly reside in Hong Kong and cities in Taiwan, in addition to Beijing. According to Figure 2-20, we found that over 50% of printers in Hong Kong and Taiwan areas provide web services (using port 80 as the default). This may be due to the printer configuration habit of users in those areas. Of course, this conclusion is reached mainly based on our preliminary analysis results. To find specific causes, we need further data support and analysis.

Figure 2-19 Distribution of exposed network printers by city

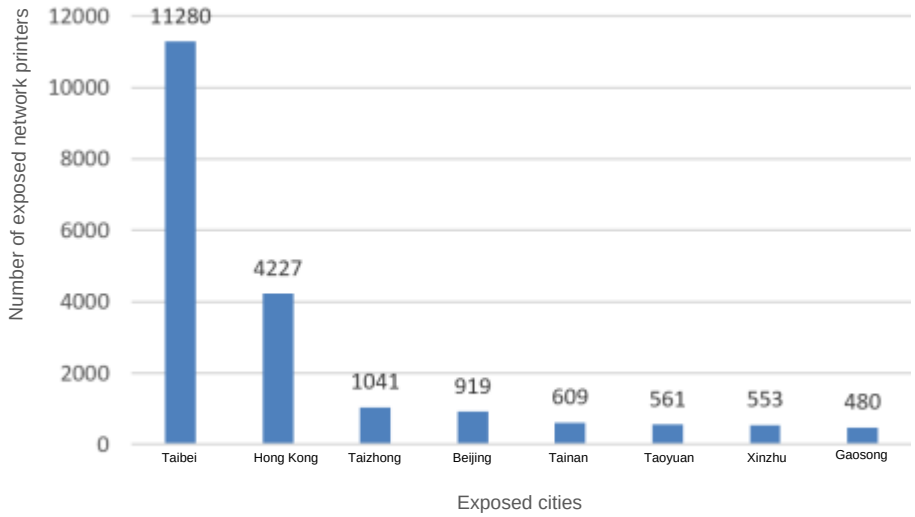
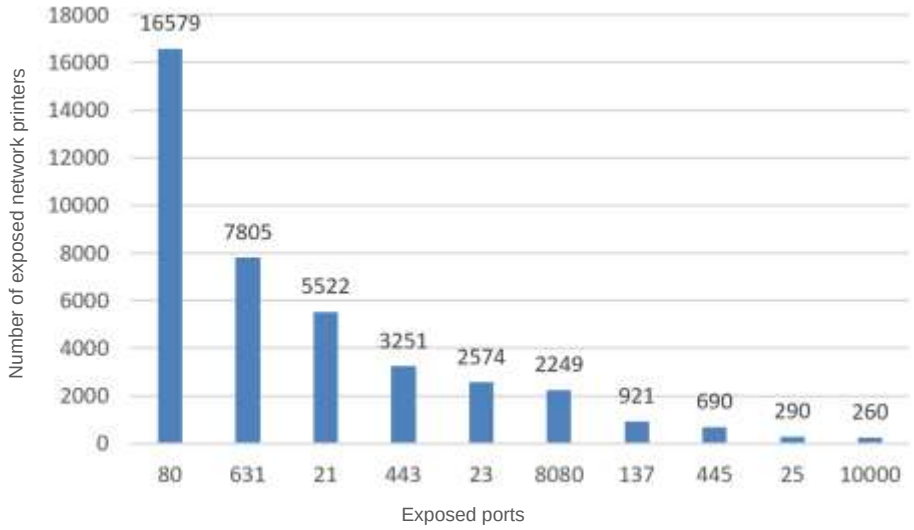


Figure 2-20 Distribution of exposed network printers by port



2.5 **Sum-up**

Massive exposure of IoT devices such as network surveillance devices, routers, and printers provide intrusion opportunities for criminals. For the previous Mirai event[6] , the hacker exploited security vulnerabilities (including weak passwords) of webcam devices for intrusion into network surveillance devices, and then planted malware to build botnets to cause network paralysis. If a large number of IoT devices are exposed on the Internet, similar security events may occur at any time, making such devices unavailable and also causing certain important information to be stolen.

3 Exposure of IoT Operating Systems in China

3.1 Introduction

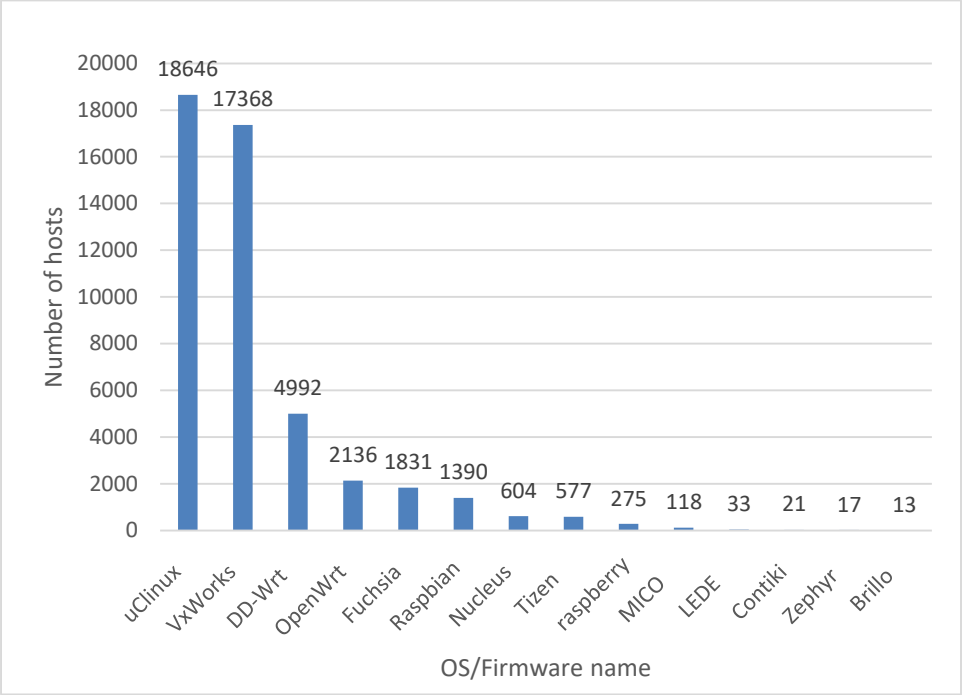
According to the *IoT Whitepaper* (2016) released by China Academy of Information and Communications Technology (CAICT), IoT operating systems are embarking on a path of innovative growth to be more scalable and interoperable. The Whitepaper classifies IoT operating systems currently available on the market into two categories: One is tailored from smartphone or PC operating systems and the other evolves from traditional embedded operating systems. The former, used in embedded devices, shows strengths in the applicable layer, but is not good at supporting underlying optimization. The latter leverages functions of traditional embedded operating systems, such as task scheduling, and incorporates the networking functionality. Some systems even integrate common wireless module drivers to meet basic needs of IoT devices for stable operations and network connectivity.

This chapter presents common IoT operating systems and analyzes the widely used ones. We hope such analysis is informative enough for readers to get a glimpse of the status quo of IoT operating systems in China.

3.2 Common IoT Operating Systems

Common IoT operating systems and firmware include uClinux, VxWorks, DD-WRT, OpenWrt, Fuchsia, Raspbian, Nucleus, Tizen, Raspberry Pi, MICO, LEDE, Contiki, Zephyr, and Brillo. Figure 3-1 shows our statistics on the use of these operating systems based on NTI data.

Figure 3-1 Comparison of common IoT OSs in the installed base



According to data in NTI, these operating systems vary a lot in the installed base number. uClinux, VxWorks, DD-WRT, OpenWrt, Fuchsia, Raspbian/Raspberry Pi, Nucleus, and Tizen each have quite a large installed base. Of these operating systems, although the search for "Tizen" returns a lot of results, most of them are retrieved because they are included in the system list of device banners, for example, "*,mac:"MacOS",win:"Windows",tizen:"Tizen",linux chrome*". This has nothing to do with the Tizen system itself or application. For this reason, our analysis does not cover Tizen. As OpenWrt, DD-WRT, and LEDE are based on the same source code of a router from Linksys, we analyze them as a whole in a separate section. Therefore, the following sections are dedicated to uClinux, VxWorks, OpenWrt (including DD-WRT, OpenWrt, and LEDE), Raspbian/Raspberry Pi, and Nucleus respectively. Other operating systems are not used so often, so they are not covered in our analysis. Besides, our analysis leaves out services and ports seldom used. In other words, we only compare ports and services exposed more than 50 times for the analysis of characteristics of some devices or operating systems.

3.3 Analysis of IoT Devices Based on Exposed Operating Systems

3.3.1 Nucleus

The development package based on the Nucleus operating system is named MTK, which reminds people of smartphones produced in China. In 2008, copycat smartphones based on the MTK platform were all the rage by delivering live broadcast of Olympic events. These smartphones were running Nucleus at that time. Now this operating system is also used by Mentor Graphics for hardware systems' power limit. People who are more concerned about the hardware and underlying systems should keep a close eye on this system.

Viewpoint 14: Devices running Nucleus generally enable HTTP and FTP services. On average, each host opens 1.59 ports to deliver the HTTP service. Hosts opening port 21 account for 75.6% of all Nucleus hosts.

From NTI, 604 host IP addresses can be found to run Nucleus. The following figures show statistics of the ports opened and upper-layer protocols running on these devices.

Figure 3-2 Statistics of ports opened on Nucleus hosts

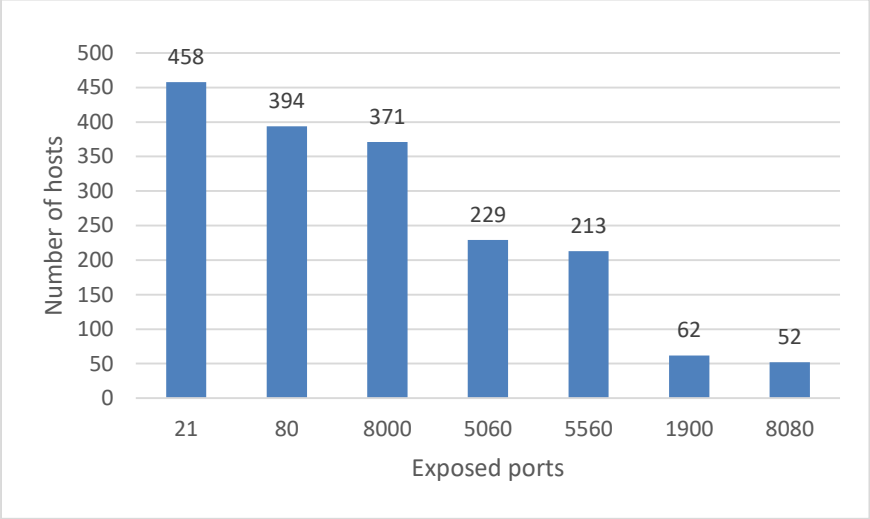
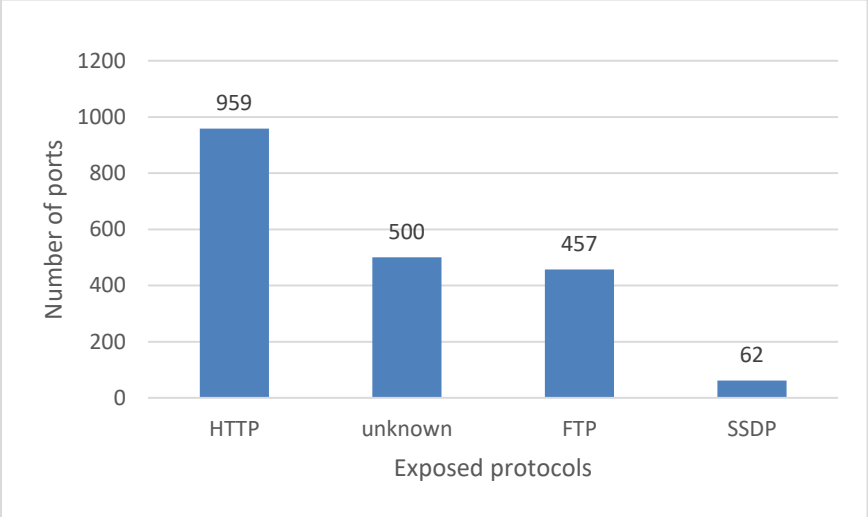
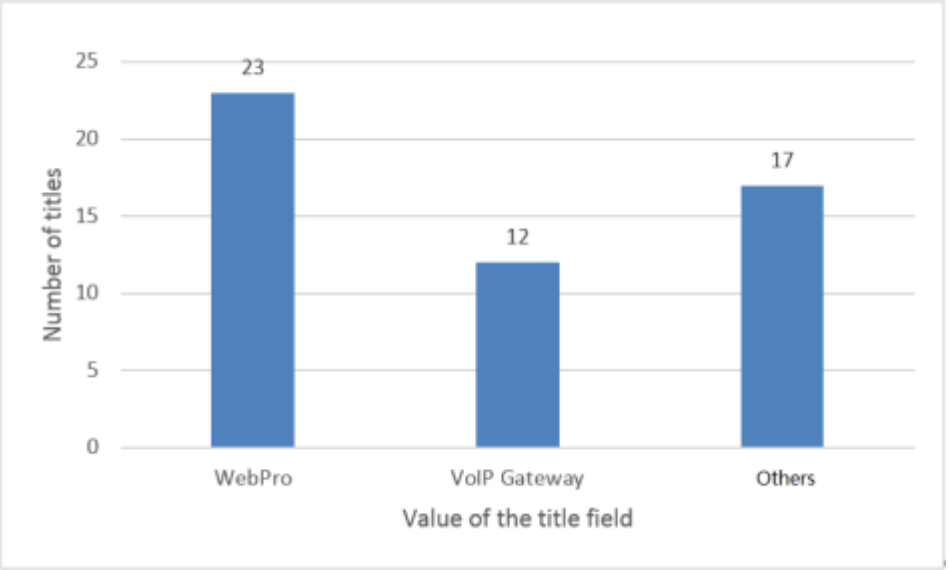


Figure 3-3 Statistics of protocols running on Nucleus hosts



The analysis of statistics provided in Figure 3-2 and Figure 3-3 finds that the number of ports opened for the HTTP service is 1.587 times that of hosts (604), and the number of ports opened for the FTP service is 75.6% of that of hosts. Besides, we did a research about the **title** field in HTTP around this type of devices. Figure 3-4 shows the outcome of our research.

Figure 3-4 Statistics of nonempty titles of HTTP pages on Nucleus hosts



As for the hosts that have enabled the HTTP service, we found 513 titles. This number is not great enough to be informative because the number of empty titles reaches 460. Among the nonempty titles, WebPro accounts for 43.4% and VoIP Gateway for 22.6%. Based on such information, we speculate that, among the 460 empty titles, some are gateway products. If access control is configured for their IP addresses, it is normal that the corresponding service cannot be accessed although the port is opened for that service. As a result, the title field is empty.

In addition, 441 banners of the FTP service contain the same message reading "*220 Nucleus FTP Server (Version 1.7) ready*", indicating that these devices have something in common, which is attributable to the same vendor or the intrinsic property of the system. Sixty hosts have the banner reading "*Nucleus/4.3 UPnP/1.0*". Considering that the number of devices enabling the SSDP service is 62, as shown in Figure 3-3, we believe that some hosts have ports opened for services of UPnP, SSDP, and the like.

3.3.2 OpenWrt/DD-WRT/LEDE

Cisco Linksys launched the Linksys WRT54G router in 2003. For this model, the company used the Linux kernel with a view of reducing the cost. However, the vendor was finally forced to make the source code public. In the wake of that, some pieces of third-party firmware based on this source code were released, including OpenWrt and DD-WRT. Later LEDE, as an embedded Linux distribution, was developed based on OpenWrt. Usually they are used on routers, but the possibility of some hobbyists using them on embedded devices, such as web cams and robots, cannot be excluded.

Viewpoint 15: Of all devices running OpenWrt/DD-WRT/LEDE, at least 13.0% do not have default settings modified. Besides, it is not unusual for these devices to use port mappings.

Figure 3-5 and Figure 3-6 show statistics of ports opened and upper-layer protocols running on devices running OpenWrt/DD-WRT/LEDE.

Figure 3-5 Statistics of ports opened on OpenWrt/DD-WRT/LEDE hosts

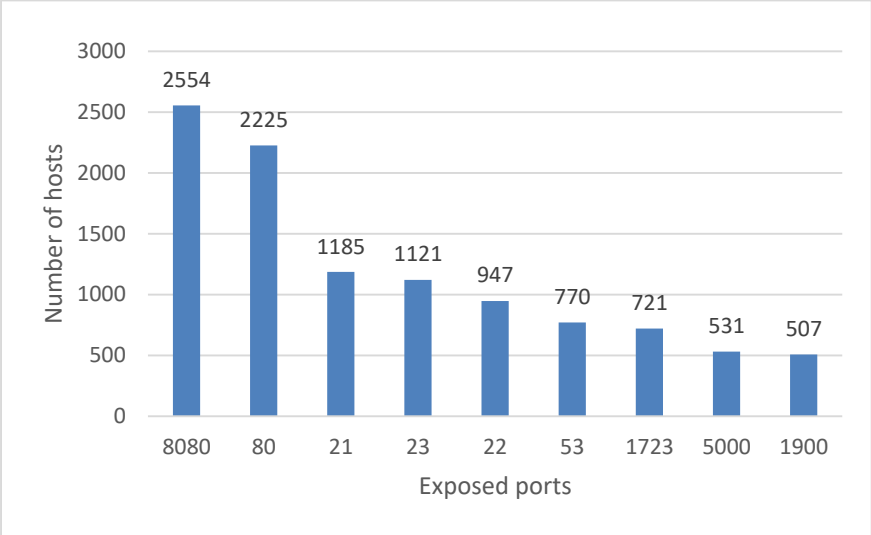
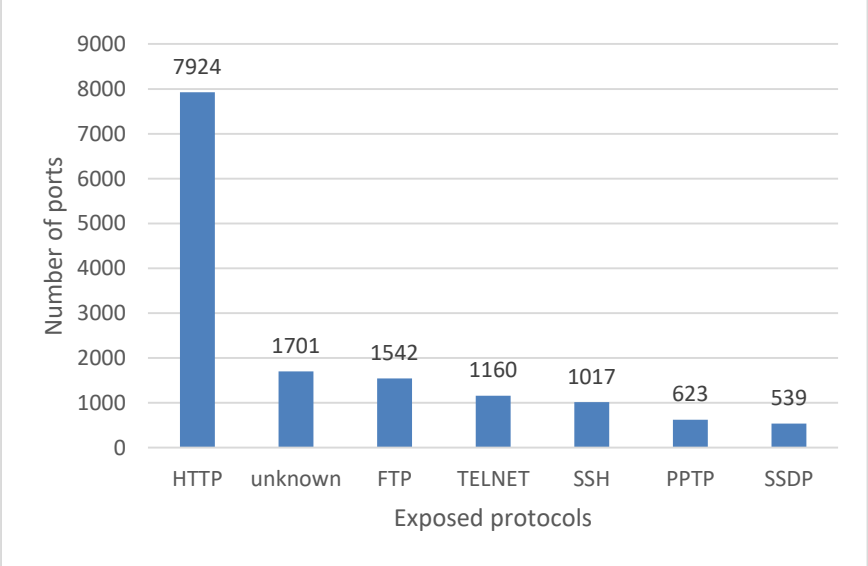


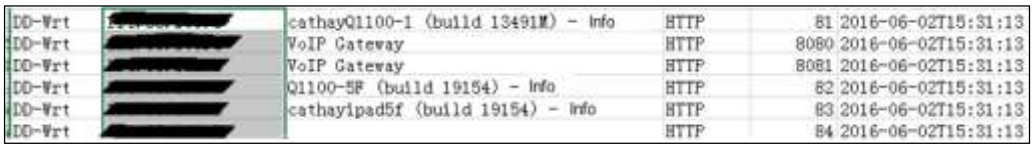
Figure 3-6 Statistics of protocols running on OpenWrt/DD-WRT/LEDE hosts



Of the 7150 OpenWrt/DD-WRT/LEDE hosts, most have ports opened for HTTP, SSH, FTP, and Telnet services. The number of ports opened for HTTP reaches 7924, 1.108 times of the number of hosts. In addition, the number for SSH and FTP also exceeds 1000 respectively. From the perspective of ports, the number of hosts having port 21 opened accounts for 16.5% and the proportion for port 22 and port 23 reaches 13.2% and 15.6% respectively.

It is worth noting that more often than not one IP address has multiple ports opened for the same service.

Figure 3-7 Ports opened for HTTP on a DD-WRT host



In Figure 3-7, a DD-WRT host has six ports opened for the HTTP service, whose title information contains four types of device. Obviously, this IP address is used by at least five devices, including two VoIP gateways. This tells us that the device type cannot be simply determined by means of scanning because NAT mappings enable one IP address to possess properties of multiple devices.

Moreover, the banner of the HTTP service delivered through the six ports contains a message like "*DD-WRT (build xxxxx="infopage"*>" (xxxxx is a five-digit number, usually indicating the compilation version of the DD-WRT firmware) or "*R6300 DD-WRT (build*". We used "build" as a keyword to search for related information and found that this field occurred 2148 times, roughly 13.0% of the total services (16,583). The search based on characters "*Basic realm="DD-WRT"*" returned 817 results, about 4.9% of the total. **This indicates that some people, when developing IoT operating systems based on the DD-WRT firmware or operating system, did not modify default settings of routers.**

3.3.3 Raspbian/Raspberry Pi

Raspbian is a free operating system based on Debian optimized for the Raspberry Pi (RPi) hardware. It comes with more than 35,000 packages. Fans of intelligent hardware are very familiar with this system. Compared with traditional embedded operating systems, Raspbian is easier to install. A user just needs to use such software as Win32DiskImager to put the official image file onto the SD card and then the system can run on RPi. Many makers are using open-source hardware, such as RPi and Arduino, to do something meaningful.

Viewpoint 16: 67.9% of devices running Raspbian have ports opened for the SSH service.

According to NTI, there are 1390 Raspbian hosts in China. Figure 3-8 and Figure 3-9 show statistics of upper-layer protocols running and ports opened on such hosts.

Figure 3-8 Protocols running on Raspbian hosts

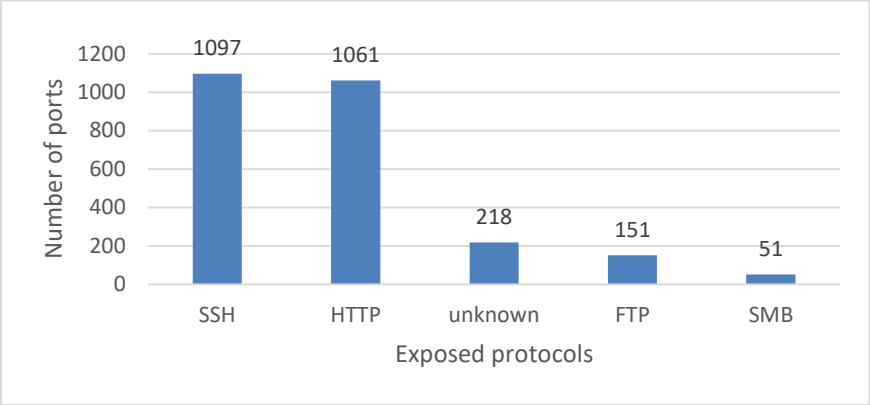
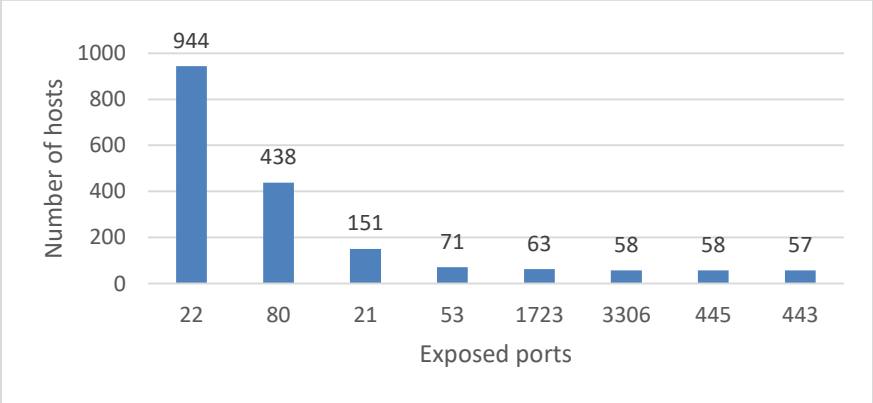


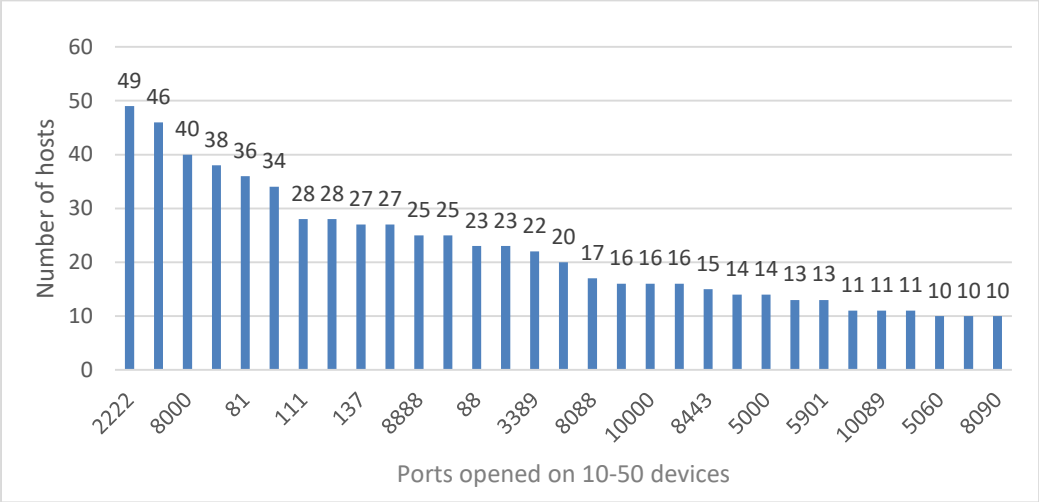
Figure 3-9 Ports opened on Raspbian hosts



According to statistics, among the 1390 hosts, 944 have port 22 opened, accounting for 67.9%. RPi, as a piece of open-source intelligent hardware, is mainly for developers and intelligent hardware enthusiasts to rapidly make product prototypes. In practice, most users do not modify the default settings of Raspbian, leaving the SSH service available for use. Therefore, a majority of devices based on RPi have the SSH service externally available.

An analysis of ports finds that most of the ports (opened on 10–50 devices) are opened for the HTTP service. This explains why the number of devices enabling HTTP varies greatly from the number of devices having ports 80 and 443 opened, as shown in Figure 3-8 and Figure 3-9. In Figure 3-10, the number of ports (including 8080, 8000, 81, 8888, 88, 8081, 82, 8088, 10000, 8443, 5000, 83, 10089, and 8090) usually opened for the HTTP service reaches 307. Plus ports 443 and 80 opened for the HTTP service, the total number exceeds 800.

Figure 3-10 Statistics of ports opened on 10–50 devices



3.3.4 **uClinux**

The original uClinux was a derivative of Linux 2.0 kernel intended for microcontrollers without Memory Management Units (MMUs). The Linux/Microcontroller Project has grown both in brand recognition and coverage of processor architectures. Today's uClinux as an operating system includes Linux kernel releases for 2.0, 2.4, and 2.6 as well as a collection of user applications, libraries, and tool chains. As an important branch of the embedded Linux system, uClinux has been used on routers, set-top boxes (STBs), personal digital assistants (PDAs), and the like.

Viewpoint 17: 98.4% of uClinux hosts enable the SSDP service.

According to NTI, there are 18,646 uClinux hosts. As too many hosts are involved, we collected data only on protocols and ports.

Figure 3-11 Statistics of protocols running on uClinux hosts

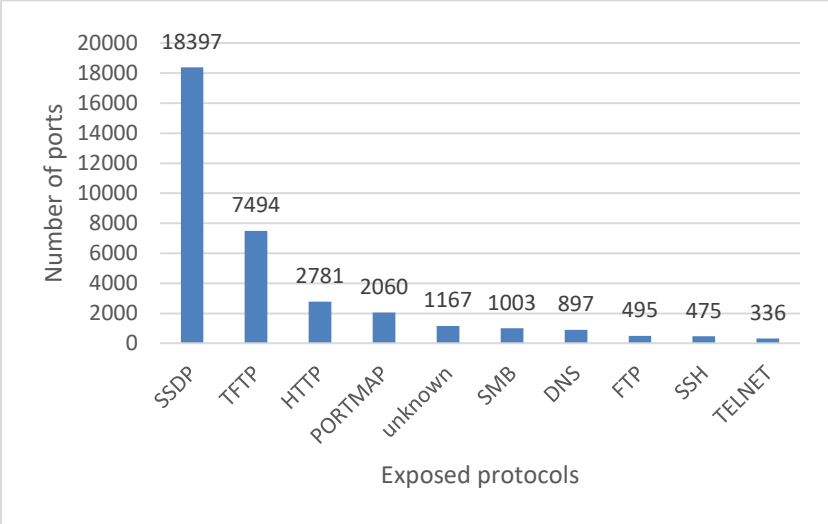
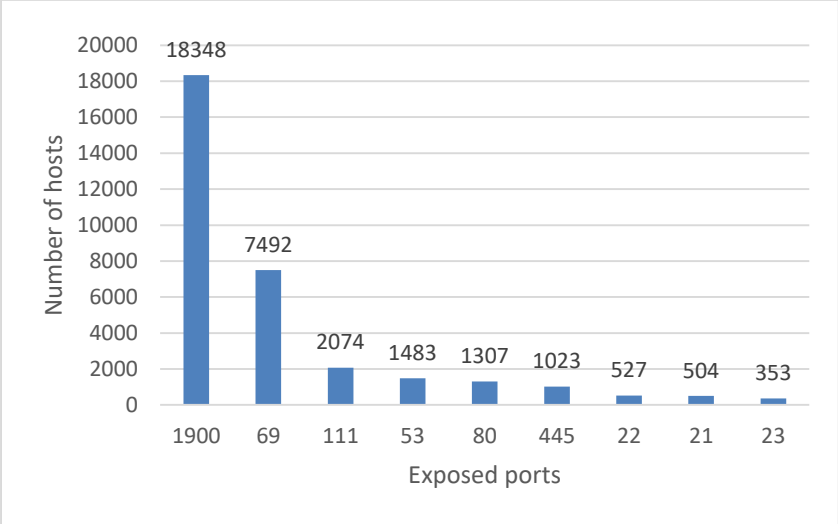


Figure 3-12 Statistics of ports opened on uClinux hosts



As there are too many ports and protocols involved, Figure 3-11 and Figure 3-12 cover only ports and protocols associated with no less than 300 hosts. Vertically, we can find that the number of devices involving protocols is in proportion to that involving ports, like the number of devices enabling SSDP and the number of devices having port 1900 opened. Horizontally, we can find the distribution of protocols and that of ports. Among 18,646 hosts, 18,348 have port 1900 opened, accounting for 98.4%, mainly for the SSDP service. In addition, among all banners, the message "*Server: uClinux/2.6.28.10 UPnP/1.0 MiniUPnPd/1.3*" appears 18,001 times. From such information, we speculate that most of these hosts are routers, which are deployed to support, by using Universal Plug and Play (UPnP), remote access between multiple devices and services on a local area network (LAN).

3.3.5 VxWorks/ WindRiver

VxWorks is an embedded, real-time operating system (RTOS) designed by Wind River, a US company, in 1993. As a universally recognized capable real-time kernel operating system in the industry, VxWorks is widely used on devices handling massive data flows, such as switches and routers, and on various precision-control devices in the aerospace field.

Viewpoint 18: Most VxWorks hosts have ports opened for HTTP, SSH, and Telnet services. On average, each host opens 1.08 ports for the HTTP service. Those devices opening ports 21 and 23 account for 67.5% and 66.9% of the total respectively.

As VxWorks is used for special purposes, its fingerprints are quite credible. NTI records 17,368 VxWorks hosts, the distribution of whose ports and upper-layer protocols is shown in Figure 3-13 and Figure 3-14 respectively.

Figure 3-13 Statistics of ports opened on VxWorks hosts

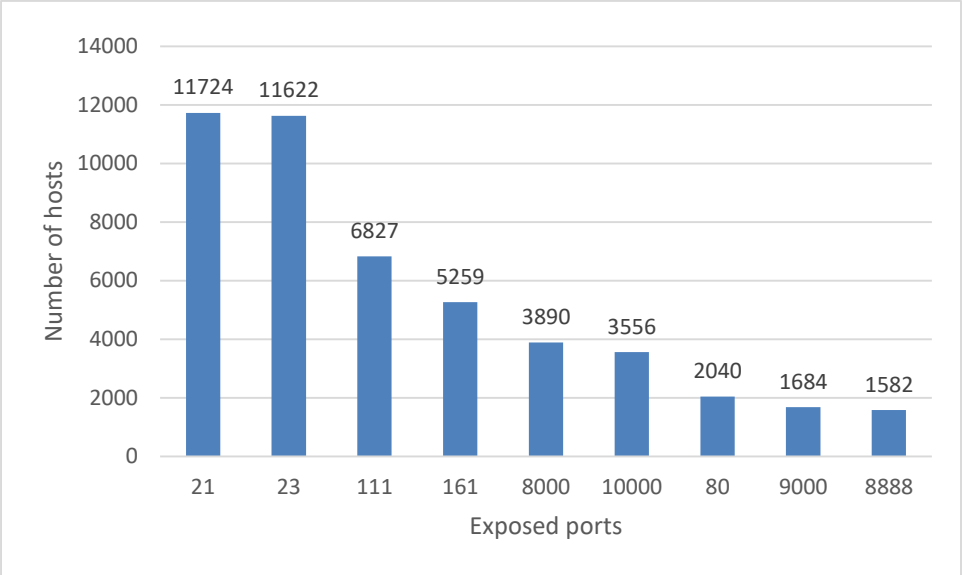
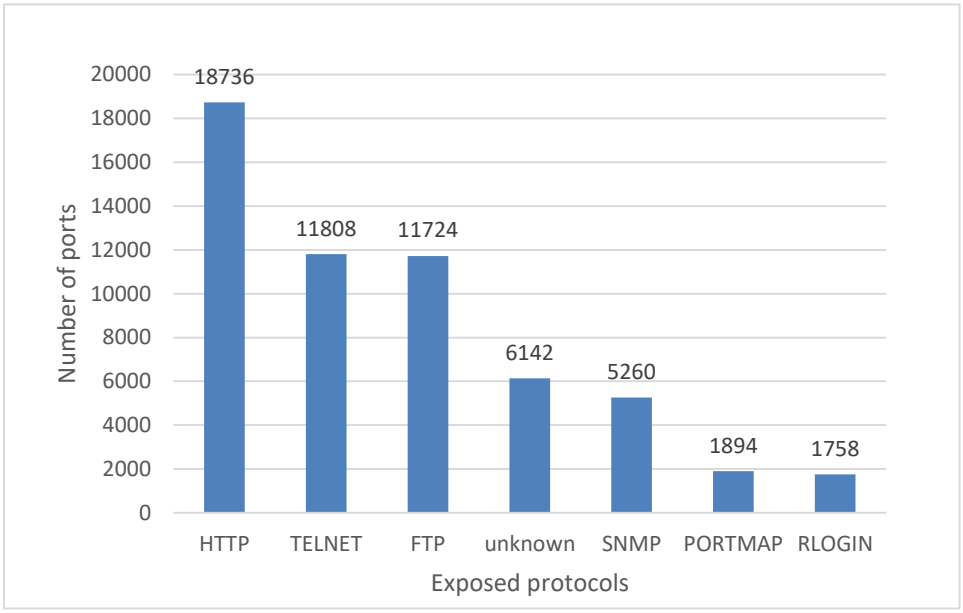


Figure 3-14 Protocols running on VxWorks hosts



From the distribution of ports, devices with port 21 opened are a bit more than devices with port 23 opened. The sum of the two accounts for about 67% of the total VxWorks hosts. Other ports are opened mainly for the HTTP service. Protocol statistics show that the HTTP service is provided through 18,736 ports, 1.079 times of the number of hosts. This means that one VxWorks host opens at least one port for the HTTP service on average. Figure 3-13 and Figure 3-14 provide the same number for FTP and port 21, and close numbers for Telnet and port 23 because the Telnet service is also provided by other ports.

Moreover, among the 17,368 VxWorks hosts, 9716 hosts have a banner containing the same message "*220 VxWorks (VxWorks5.5.1) FTP server ready*", and 4758 hosts have the message "*VxWorks SNMPv1/v2c AgentVxWorks SNMPv1/v2c Agent*" or "*VxWorks SNMPv1/v2c Agent*" in their banner.

3.4 Conclusion

The preceding sections analyze some common IoT OSs, including Nucleus, OpenWrt, Raspbian, uClinux, and VxWorks in terms of the exposed ports and application-layer protocols. Through analysis, we have the following findings:

1. Devices running one of these five operating systems have some common signatures, which are contained in the banner of services. For example, VxWorks hosts deliver the message "*220 VxWorks (VxWorks5.5.1) FTP server ready*" in the banner and uClinux hosts deliver the message "*Server: uClinux/2.6.28.10 UPnP/1.0 MiniUPnPd/1.3*" in the banner.
2. Some devices are deployed with default system settings for connection to the Internet. For example, the title field of HTTP in the DD-WRT firmware provides information like "*DD-WRT (build xxxxx="infopage"*>".
3. Sometimes an IP address (device) is associated with multiple intranet IP addresses (devices). This is probably because multiple devices are mounted to a router via UPnP. As a result, one IP address delivers different services with different device IDs because

the NAT mapping makes it possible for an IP address to embody combined properties of multiple devices.

Other operating systems, such as Brillo, TinyOS, LiteOS, Linino OS, Ostro, FreeRTOS, Contiki, MICO, and Zephyr, are not analyzed here because they have much smaller installed bases according to results returned by cyberspace search engines.

4 Sum-Up

Based on scanning data of NTI, Shodan, and ZoomEye, we analyzed IoT assets located in the Chinese territory from two perspectives: One is the distribution of various devices on the Internet and the other is the exposure of IoT operating systems on the Internet.

Owing to the limited time and energy, we cannot guarantee that our analysis covers all types of devices and all operating systems in use. And even for the covered device types and operating systems, we cannot safely say that all related data is 100% accurate. In spite of this, we tried our utmost to ensure the comprehensiveness and accuracy of data by basing our research on the comparison and analysis of data from three search engines instead of relying only on one search engine. Then, our purpose is to call people's attention to the necessity and urgency of IoT protection by revealing the exposure of IoT devices on the Internet. In this sense, a few omissions or some noisy data will not prevent readers from understanding our viewpoints presented in this article.

This article dwells upon such IoT devices as video surveillance devices, routers, and printers. In future, we will analyze the exposure of more devices and may update data provided here as necessary.

Based on our findings, we recommend users and vendors to do the following for their IoT devices:

- Users:
  - Enhance security of user names and passwords by changing initial passwords and weak passwords.
  - Disable unused ports such as ports 21 (FTP), 22 (SSH), and 23 (Telnet).
  - Upgrade device firmware in time.
- Vendors:
  - For the first use of devices, force users to change the initial password and check the complexity of passwords set by users.
  - Provide an automatic online upgrade option for device firmware to reduce the exposure of networked devices to security risks.
  - Provide default settings according to the principle of opening the fewest ports required to reduce the possibility of ports exposed on the Internet.
  - Set access control rules to strictly control external access from the Internet.

References

[1] NSFOCUS Threat Intelligence (NTI), https://nti.nsfocus.com/.

[2] Shodan, https://www.shodan.io/.

[3] ZoomEye, https://www.zoomeye.org/.

[4] Router Vigilante: "Malware" Linux.Wifatch, http://www.freebuf.com/news/80510.html.

[5] Mysterious Malware Wifatch Developer Identified, http://www.aqniu.com/industry/10656.html.

[6] Smart Devices Threatened by a Flood of Vulnerabilities, http://www.cctime.com/html/2016-10-25/1232231.htm.

[7] 1.37 Billion Identity Leak Story, http://mt.sohu.com/20170307/n482644552.shtml.

[8] How to Access the FTP Server of Dual-Band Wireless Routers, 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] IoT Whitepaper (2016), China Academy of Information and Communications Technology.

[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] A Promising Market for Printers in China, http://www.qianzhan.com/analyst/detail/220/150807-0da16321.html.

[15] 600,000+ IoT Devices Infected with Mirai Worldwide, http://www.kejixun.com/article/161020/237548.shtml.

[16] Smart Printers Will Be a Trend, http://column.iresearch.cn/b/201607/774585.shtml.

[17] Xiaomi Has Sold 10 Million Mi Wi-Fi Routers That Connect to Over 120 Million Devices, http://tech.ifeng.com/a/20170119/44533970_0.shtml.

[18] 360 Ranked First in First Half of 2016 for Its Wi-Fi Routers That Experienced an Increase of 143% in Sales Volume, http://network.pconline.com.cn/821/8217402.html.

[19] Uniview Holds the Third Largest Market Share in China in 2013 Thanks to Its Full Range of Products, http://news.c-ps.net/article/201409/212461.html.