2019

Cybersecurity Insights

NSFOCUS

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

1

Executive Summary

2019 witnessed more intense challenges in global political and economic orders. Restricted by various conventions, agreements, and protocols, traditional military means are now the last resort. In this context, attacks on the financial sector and on the cyberspace become the first choices for rival countries to try on their modern military strategies. Predictably, these attacks will probably become regular approaches in the future. By the time when the *2018 Cybersecurity Insights* was released, the following trends had taken shape regarding cybersecurity: The window between the discovery of a vulnerability and the effective exploitation of this vulnerability was shortened; the DDoS attack size steadily grew; emerging threats like those from the Internet of Things (IoT) rose sharply; such malware as backdoors, cryptojackers, worms, trojans, and botnets were still active. When it comes to information disclosure, the AcFun website was hacked, leading to a leak of nearly 10 million pieces of user data; India's Aadhaar (India's national ID database) number leak affected 1.1 billion citizens. Information disclosure events have hit record highs for six years in a row since 2013. The four enterprises, namely Facebook, Equifax, British Airways, and Marriott International, together were fined approximately USD 9 billion for privacy and information leaks, more than the aggregate market value of the cybersecurity industry in China in that year.

In the past few years, the cybersecurity awareness has been greatly improved. Related events are attracting attention from not only industry insiders but also all other people that the media can reach. Major cybersecurity events, including ransomware attacks, DDoS attacks, and IoT compromise, could affect social and economic activities in various sectors, stressing out IT professionals and security teams. The large-scale power outages in Venezuela and Ukraine, Iran's missile launchers being paralyzed in a hack, and other incidents targeting a country's critical infrastructure have changed people's perception of cybersecurity, making them realize that cyberattacks are not just for personal showoffs and financial pursuits, but can impact the national security. This leads them to better understand a united system of land, sea, air, space, and cyber forces. Following these incidents, Russia tested its unplugged Internet and the USA unveiled a spending bill that includes millions of dollars for election cyber security. All these newsmakers keep opening people's eyes and support the statement that "the security of the cyberspace is an integral part of national security".

At the same time, governments around the world have put in place various measures to address

cybersecurity.

In 1993, the USA issued the *National Information Infrastructure: Agenda for Action*. Two years later, it made the concept of information warfare known to the world. Since then, in over 20 years, the USA has developed and updated many policies, laws, and regulations around the country's defense capabilities in the cyberspace. Well-known examples of these policies, laws, and regulations are *Joint Publication 3-13: Information Operations, USA Patriot Act, Comprehensive National Cybersecurity Initiative* (CNCI), *2015 DoD Cyber Strategy, National Security Strategy* (2017), *2018 DoD Cyber Strategy, and National Cyber Strategy* (2019). Besides, the country has carried out various cyber offensive and defensive exercises over this period.

In the wake of the *General Data Protection Regulation* (GDPR) taking effect on May 25, 2018, the European Union (EU) greenlighted the *EU Cybersecurity Act* in March 2019, in a bid to build a general cybersecurity certification framework. In April 2019, the North Atlantic Treaty Organization (NATO) conducted the Locked Shield real-time cybersecurity exercise, with an eye to cementing the cooperation between countries in military and civilian areas.

In the future, digitalization and globalization will permeate through every corner of the world, bringing benefits for all. Compared with the report released in 2018, our *2019 Cybersecurity Insights* adds the "Security Threats in the IPv6 Environment" chapter, noting that the IPv6-based Next Generation Internet (NGI) will become the cornerstone to support the rapid development of cutting-edge technologies and industries.

Where there are vulnerabilities, there are security events. This report compares the number of CVE vulnerabilities changing over a 10-year period from 2010 and lists top 10 vulnerabilities in 2019. Besides, trends of server, IoT device, and common application exploits are described respectively.

On the basis of reports released in previous years, we added a lot of new contents to expand the coverage of the 2019 report. Focusing on the security landscape and biggest trends in 2019, the report is aimed at delineating cybersecurity in an all-round manner, providing readers with insights into cybersecurity so that they can make accurate predictions and informed decisions when considering deploying related protections. Also, this report reminds readers to keep a close eye on the evolution of security risks and align their operations with security requirements in the new context.

2

Key Findings

Key Findings

1. [Vulnerabilities] 2019 saw a steady increase in high-risk vulnerabilities and in Internet of Things (IoT) vulnerability exploits. Of server-related vulnerabilities, web vulnerabilities stole the spotlight and the Windows remote desktop vulnerability CVE-2019-0708 had a far-reaching impact.
2. [Malware] Ransomware and cryptojacking malware were two most active types of malware in 2019. In this year, ransomware presented itself as an effective tool readily available for hackers to attack a wide range of targets and to make a killing. In the meantime, the trend of industrializing ransomware became increasingly obvious. As for cryptojackers, those for mining Monero were still popular. Besides, cryptojackers provided more compromise options, characterized by modular design and capable of hiding themselves.
3. [Malicious traffic] 2019 witnessed a slew of conventional web attacks , most of which were launched by exploiting deserialization vulnerabilities. Remote code execution (RCE) vulnerabilities requiring no authentication were most favored by hackers. The security of third-party databases should be put on top of the agenda. The time to exploit website vulnerabilities was further accelerated and web masters should be more mindful of website security.
4. [Malicious traffic] DDoS attackers were powered by mature techniques. Multi-vector volumetric attacks posed a greater challenge to defense operations. Of those initiating DDoS attacks, recidivists were rather dangerous, especially active IP gangs, which require continuous attention and should be effectively blocked. At the same time, IoT devices were making more presence in DDoS attacks and IoT-based malware families contributed an increasingly large proportion of attacks, calling for more efforts to be made in IoT security governance.
5. [Malicious traffic] In 2019, cryptojacking was on the rise, a direct result of the booming cryptocurrency market. Monero was still the most coveted prey for attackers. Small and medium-sized enterprises doing traditional business were most frequently attacked for this purpose. Ports ranging from 3000 to 3999 were often used by cryptojackers. Another thing to note is that web-based cryptojacking remained popular. Among Alexa's top 1 million websites, over 2000 were planted with cryptomining scripts.
6. [IoT] In 2019, over 30 types of IoT vulnerability exploits were captured, most of which targeted

RCE vulnerabilities. IoT devices, especially cameras and routers, were the major targets of Telnet-based weak password cracking attacks. UPnP/SSDP- and WS-Discovery-related threats were so rampant that all players on the defensive side, including security vendors, service providers, and telecom carriers, should remain vigilant of related attacks.

7. [IPv6] Globally, the past years have witnessed an ever increasing adoption of IPv6. Amid this trend, IPv6-related vulnerabilities are on the rise. These vulnerabilities exist because of not only new fields and new protocols introduced to IPv6 packets but also the use of transitional techniques that have inherent security issues. In current IPv6 attacks, traffic was mostly initiated against the transport layer and application layer. Backdoors, cryptojackers, and trojans were most frequently used in these attacks. From the perspective of services attacked, web-related services attracted the most attention from hackers.

3

Overall Situation

3.1 Attack Type Distribution

In terms of attack types [1], DDoS attracted the largest proportion (35%) of malicious IP addresses. Other types that malicious IP addresses were most interested in included spam, botnets, and scanning.

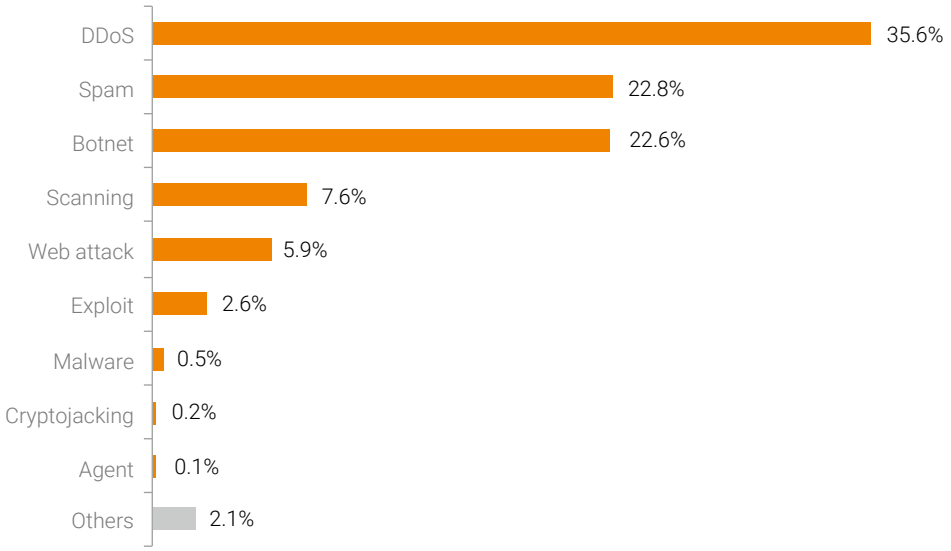


Figure3-1 Attack type distribution

Of all malicious IP addresses, 15% exploited more than one attack vector. According to our observation of such IP addresses, there are certain conversion patterns between different types of attack sources:

- An IP address sending spam has an over 90% chance of performing malicious scans over the Internet. Malicious scanning and spam both need large quantities of hosts. Therefore, the same batch of resources may be used for these two purposes at the same time.
- Botnet hosts are linked with various attacks. The most common one is malicious scanning, followed by spam and phishing.
- Web attack sources have a 50% chance of attempting more sophisticated exploitation

1 As an IP address may launch more than one type of attacks, the sum of all percentages indicated in the following figure is greater than 100%.

operations. Web attacks are quite simple. This means that attackers can easily exploit web vulnerabilities to obtain low privileges or other sensitive information and then use the collected intelligence for further penetration and exploitation.

- Of the controlled IP addresses involved in DDoS attacks, quite a large proportion have engaged in cryptomining. Attackers are profit-driven. They tend to make full use of resources on hand. When it is not time for DDoS attacks, they will leverage hosts under their control to mine cryptocurrency, thus maximizing the chance of making easy money.

3.2 Geographic Distribution

In terms of the geographic distribution, attack sources, namely, IP addresses, were mainly distributed in China, the USA, Vietnam, India, and Brazil in the global sphere. When it comes to China, such provinces and regions as Guangdong, Shandong, Jiangsu, Zhejiang, and Taiwan were home to the largest number of such IP addresses.

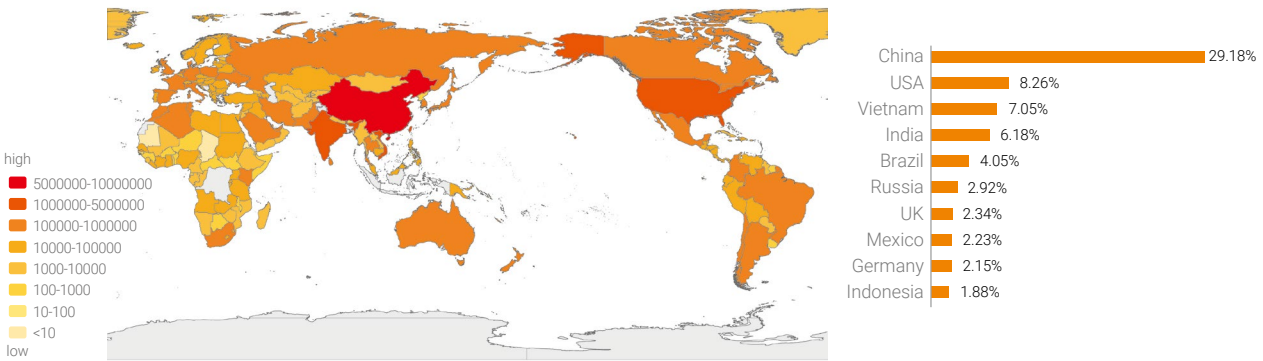


Figure 3-2 Global distribution of source IP addresses

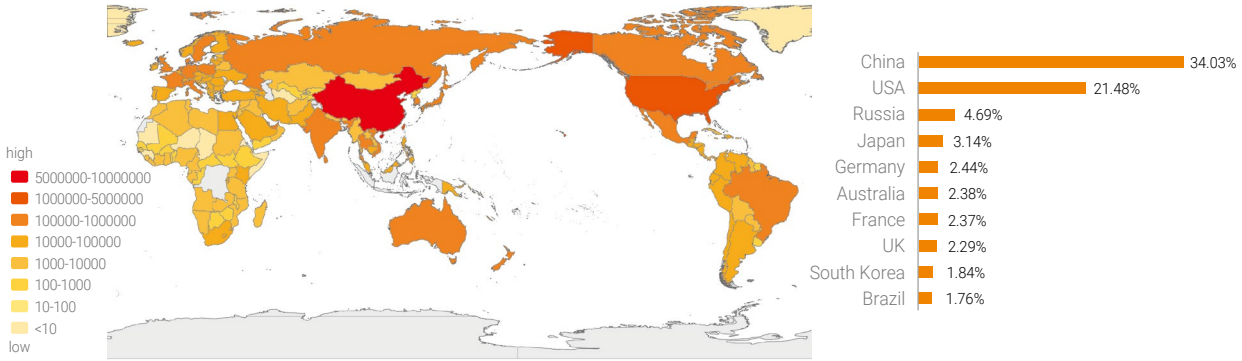


Figure 3-3 Global distribution of target IP addresses

4

Vulnerability and Exploit

4.1 Vulnerability Trend

By November 27, 2019, the National Vulnerability Database (NVD) had recorded 11,633 CVE vulnerabilities disclosed in 2019, including 6549 high-risk ones. The annual total number decreased year by year in the past three years compared with 15,881 in 2017 and 15,861 in 2018, but that of high-risk ones was on the rise.

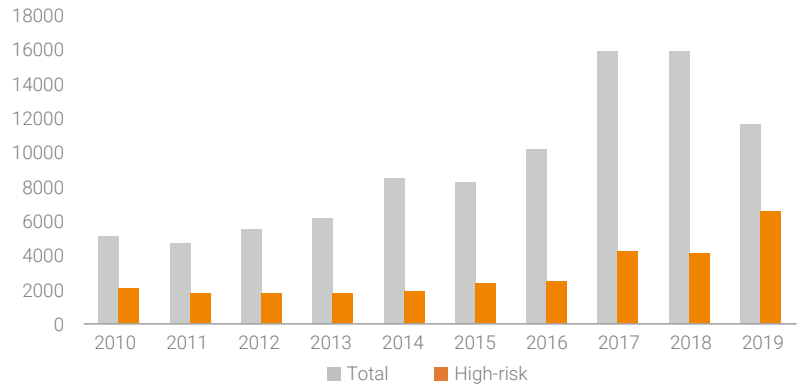


Figure 4-1 Annual CVE Vulnerabilities in the Past Decade

According to the classification criteria of Common Weakness Enumeration (CWE), the following categories of vulnerabilities took top 10 spots on the 2019 list.

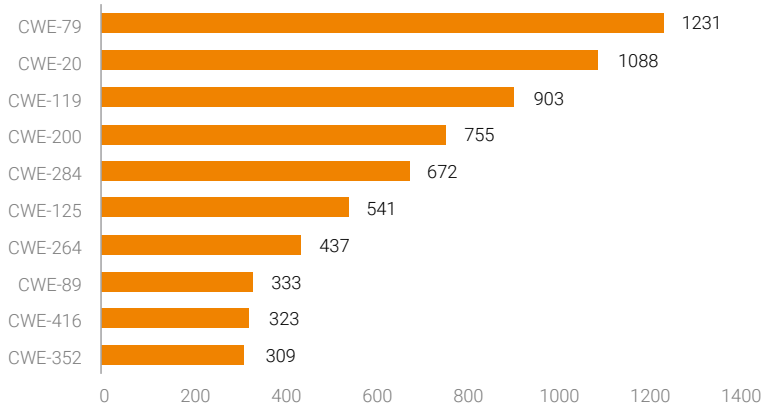


Figure 4-2 2019 CWE Top 10 Vulnerability Categories

CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer), CWE-125 (Out-

of-bounds Read), and CWE-416 (Use After Free) are all related to out-of-bounds memory operations, together contributing 1767 vulnerabilities, which could be exploited to execute arbitrary code. These categories are often seen in browsers and Office software and also the major targets and weapons of APT attackers. CWE-264 (Permissions, Privileges, and Access Controls) and CWE-284 (Improper Access Control) are related to privileges, under which 1109 vulnerabilities were disclosed in 2019, mainly in server operating systems, database applications, and some widely adopted open-source content management systems (CMSs). Traditional web attack methods are never forgotten. CWE-79 (Cross-site Scripting (XSS)), CWE-89 (SQL Injection), and CWE-352 (Cross-Site Request Forgery (CSRF)) are often seen in servers and web applications, which could allow attackers to tamper with website data by injecting malicious scripts into web pages. CWE-200 (Information Exposure) is another category that has quite a few vulnerabilities found in the past year. By exploiting such a vulnerability, an attacker could obtain sensitive information, such as system configuration information and database information, which may aid in further attacks.

When it comes to topical vulnerabilities in 2019, the Microsoft remote desktop service vulnerability naturally jumps into our minds. On May 14, 2019, Microsoft released an emergency security alert, announcing remediation of a critical vulnerability (CVE-2019-0708) in Windows Remote Desktop Protocol (RDP). This vulnerability does not require authentication or user interaction and so is "wormable". Specifically, this is a use-after-free vulnerability. When an RDP connection is set up, the RDP server creates an MS_T120 static virtual channel by default, which is bound to the 0x1F channel index. Then, if the RDP client requests binding of the MS_T120 channel to a specified channel index, the MS_T120 channel will be bound to two indexes, leading to two independent references. This way, when the client requests freeing of the MS_T120 channel, the related references will be deleted to free the object. The truth is that, when the RDP connection is closed, the MS_T120 channel of 0x1F will also be freed. As this object space has been freed before, referencing it again will trigger the use-after-free vulnerability.

On September 7, 2019, Metasploit made the exploit module of this vulnerability, cve_2019_0708_bluekeep_rce.rb, known to the public. This module targets 64-bit Windows 7 and Windows Server 2008 R2. From the options shown in the following figure, obviously, an attacker could launch a targeted attack by setting RHOSTS, RPORT, and target. By far, our devices have generated 56,827 alerts on attacks

launched by exploiting this vulnerability.

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT            3389             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
```

4.2 Exploit Trends

4.2.1 Server Exploits

Server vulnerabilities mainly reside in system services and programs that run on a server to support or deliver network management and actual business. Related exploits mainly target web servers, including Apache, Tomcat, and WebLogic. Most websites hold valuable information, such as credit card numbers, email addresses, and passwords, making them attractive targets for attackers.

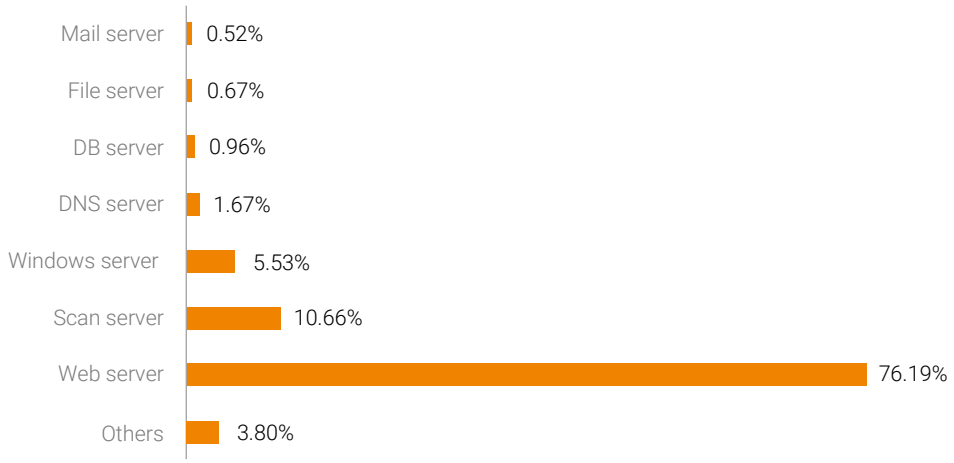


Figure 4-3 Types of servers targeted by exploits

What comes in second is the scan server, followed by the Windows server. The related exploits mainly target such network services as the Server Message Block (SMB), Remote Procedure Call (RPC), Internet Information Services (IIS), and RDP. The exploit of the MS17-010 SMB remote vulnerabilities, since its disclosure by Shadow Brokers, has been integrated into a number of worm families. In the past two years, this exploit has topped the list of all Windows server-related exploits detected by our devices. Unlike previous years, 2019 saw a breakout of RDP exploits, represented by those targeting the CVE-2019-0708 vulnerability.

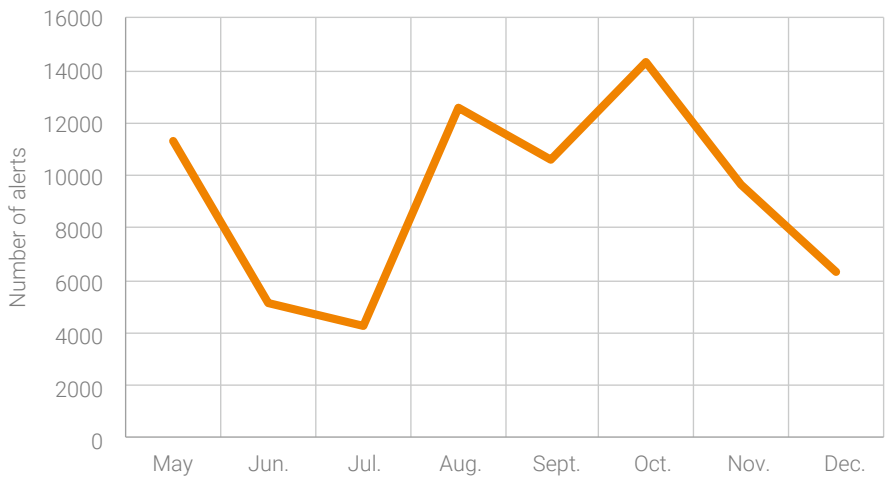


Figure 4-4 Monthly exploits targeting the CVE-2019-0708 RDP RCE vulnerability

4.2.2 Application Exploits

Application software provides document, multimedia, host management, and other functions. Typical examples of such software are clients (such as browsers and email clients), antivirus software, office suites, Flash players, and PDF readers. Exploits targeting applications are conducted by delivering malicious programs via phishing emails that contain malicious links or attachments. Once a user clicks such a link or opens such an attachment, the vulnerability in the target program will be triggered, causing the device to be infected and information to be disclosed.

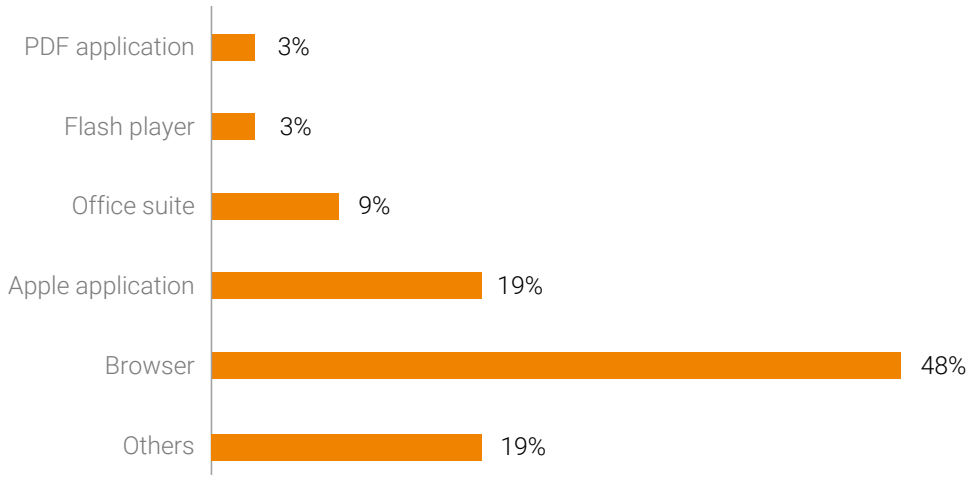


Figure 4-5 Types of applications targeted by exploits

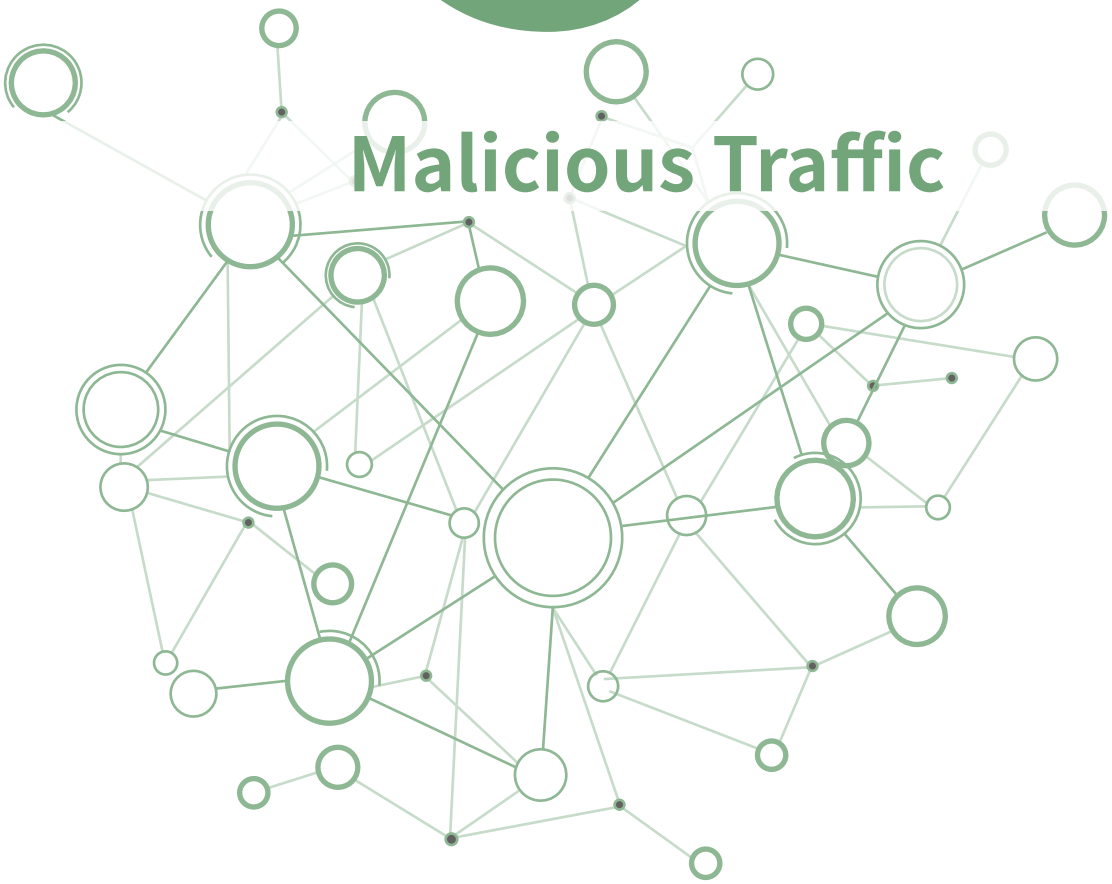
Of all application exploits, browser exploits accounted for 48%, most of which targeted Microsoft's Internet Explorer/Edge and Google Chrome. Vulnerabilities in browsers are mainly caused by improper handling of memory objects by scripting engines, including JavaScript, VBScript, WebKit, and the newcomer WebAssembly.

Exploits of vulnerabilities in Apple applications increased to 19% from 0.6% in 2018. On August 29, 2019, Google's security team Project Zero disclosed five exploit chains and 14 related vulnerabilities in Apple systems from iOS 10 to the latest iOS 12. From the system time, it can be inferred that these attackers had been active for at least two years.

Office vulnerabilities are one of hackers' favorite targets. Most APT groups also choose to exploit high-risk vulnerabilities in Office. Most security events breaking out in the past few years have been found to exploit the OLE2Link object logic vulnerability, EQNEDT32.EXE vulnerability, and Encapsulated PostScript (EPS) vulnerability. Besides, hackers could attack their targets via a Word attachment that contains malicious Flash animations. Though small in number, vulnerabilities in Flash can pose a serious threat as they are frequently exploited. What is worse is that related exploit techniques have been further improved since Hacking Team disclosed the two zero-day vulnerabilities, CVE-2015-5122 and CVE-2015-5199.

5

Malicious Traffic



5.1 Web Threats

5.1.1 Web Attack Trend

Websites, which enterprises or individuals use to provide services for users, are usually the first choice of hackers during attacks. Web attacks in 2019 clung to traditional patterns and methods, including server information disclosure, resource leeching, cross-origin resource sharing (CORS), SQL injection, and cookie poisoning, which together accounted for 89% of web attacks. Given their high popularity, these traditional methods will continue to be a top concern for defenders.

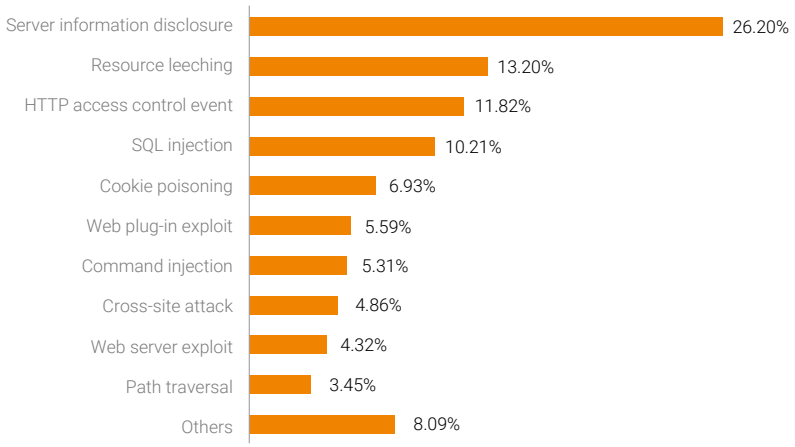


Figure 5-1 Proportions of different types of web attacks

Compared with the previous year, 2019 was a stable year for web framework/middleware attacks, though attacks targeting the ThinkPHP framework did rise significantly as a result of multiple vulnerabilities reported in mainstream 3.x and 5.x versions. This year, no new high-risk vulnerabilities were reported in Apache Struts 2. However, as this framework contains a lot of legacy vulnerabilities, it still suffered the most attacks in the past year, ranking No. 1 for three straight years on the list of web frameworks under attack. Mainstream web middleware, including Apache Tomcat, Microsoft IIS, and Oracle WebLogic Server, was still frequently attacked. This is because these products have a large installed base and carry a great number of applications, thus becoming a magnet to hackers, who are poised to exploit any vulnerabilities disclosed.

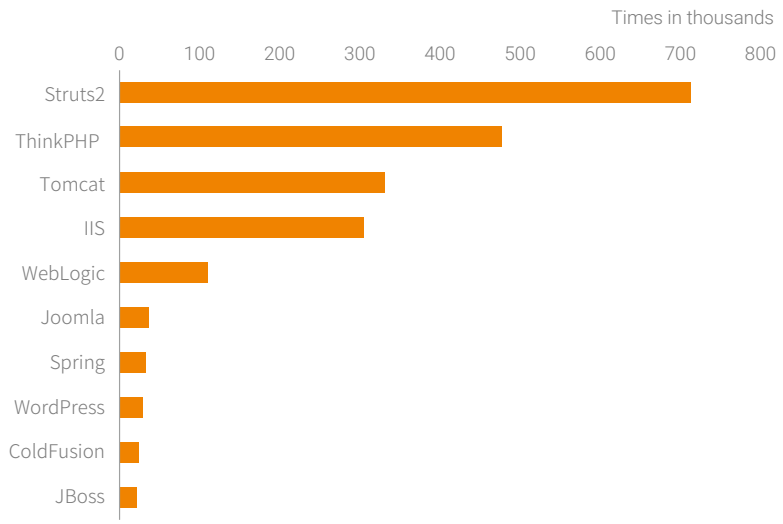


Figure 5-2 Top 10 web frameworks/middleware under attack

5.1.2 Web Exploits

Deserialization vulnerabilities are still frequently exploited for web attacks and special attention should be paid to the security of mainstream frameworks.

This section describes web vulnerabilities that had an extensive impact in 2019:

1. WebLogic

In 2017, Oracle released an official patch that fixed the XMLDecoder vulnerability (CVE-2017-10352) in WebLogic Server. This patch was evaded twice by exploits targeting two vulnerabilities (CVE-2019-2725 and CVE-2019-2729), sparking new rounds of WebLogic-targeting attacks. The two vulnerabilities reside in components built in WebLogic and could be exploited without authentication. With carefully crafted XML data in the SOAP format, an attacker could trigger the two vulnerabilities via an HTTP request. The two vulnerabilities, due to the high exploitability, are favored by hacking groups. According to statistics, after Oracle released the official security patch in April, the proof of concept (PoC) of the vulnerability (CVE-2019-2725) was publically available, encouraging a marked increase in attacks against WebLogic. Later, researchers discovered that the security patch was circumvented by an exploit (CVE-2019-2729). Obviously, the official remediation did not work, resulting in attacks reaching the culmination in May.

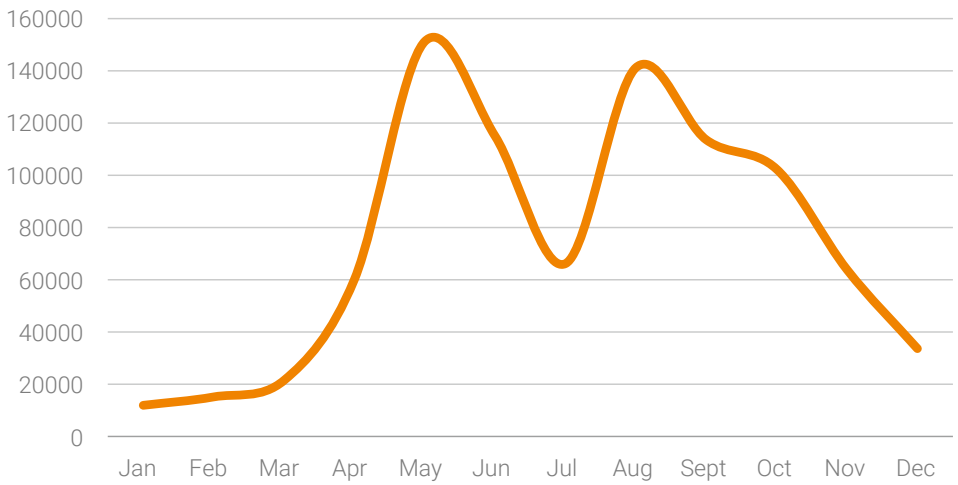


Figure 5-3 Trend of WebLogic-targeting attacks in 2019

2. JSON framework

In 2019, vulnerabilities were frequently disclosed in third-party JSON libraries for Java. Most JavaWeb applications have employed the efficient third-party JSON libraries for JSON data parsing, but version upgrades of the libraries are often overlooked during the running of applications. Thus, particular attention should be given to the security of third-party libraries.

(1) Fastjson is an open-source JSON parsing library provided by Alibaba. This library works efficiently and therefore is widely used. On one hand, security issues with Fastjson due to untrusted deserialization have been fixed multiple times since 2017. On the other hand, related remediation patches were evaded constantly. In 2019 alone, 36 blacklisted entries were newly added for Fastjson to prevent insecure deserialization, suggesting the continuously escalating battle between remediation and evasion. Users should check the official security bulletins from time to time to get the related patch as soon as possible and strictly control the switch of the AutoType function, leaving it disabled.

(2) Likewise, the Jackson library lacks proper sanitization of user input, which could be exploited for malicious parsing of related classes, thus leading to arbitrary code execution. In 2019, six

blacklisted classes were newly added for Jackson. Users should upgrade to the latest version as soon as possible to prevent this kind of attacks.

3. Others

(1) ThinkPHP 5.x was reported to contain a remote code execution vulnerability requiring no authentication to exploit. This vulnerability had an extensive impact in China as a large number of websites were hit by hackers through injection of malware such as cryptomining scripts and malicious trojans.

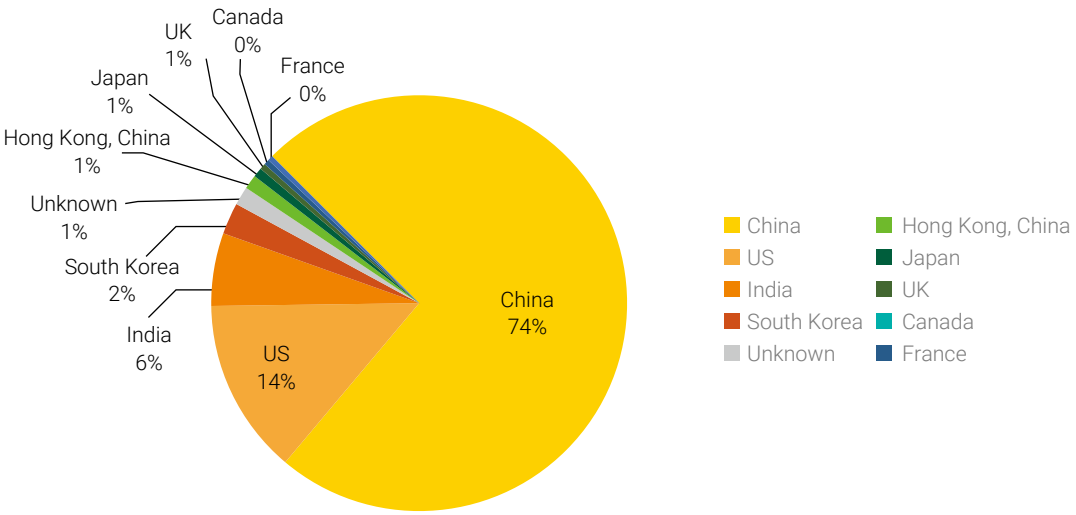


Figure 5-4 Top 10 countries with most attack source IP addresses

From the above figure, we can see that 75% of attackers hitting ThinkPHP were sourced from China. This is because the ThinkPHP framework is more popular in China, according to the distribution of attack source IP addresses.

Nearly 50% of victims were from Beijing, followed by Shanghai, Fujian, and Jiangsu provinces.

(2) Jenkins is the most popular application for continuous integration. At the end of 2018, a remote code execution vulnerability requiring no authentication to exploit was disclosed in Jenkins. Since then, the popular Script Security plug-in installed by default in Jenkins has been

repeatedly reported to contain a sandbox bypass issue. In response to such issues, security updates have been released, with the latest one seen in November 2019. As Jenkins is widely used in intranets, administrators should keep a close eye on security issues with Jenkins and its plug-ins.

(3) Apache Solr was reported to contain five high-risk vulnerabilities, including deserialization, command injection, denial-of-service, and template injection vulnerabilities. Obviously, close attention should be paid to the security of Apache Solr, a widely used indexing/search integration application.

(4) Traditional office automation (OA) systems have gained renewed attention. Weaver OA, Seeyon OA, and Office Anywhere were found to contain high-risk vulnerabilities that were widely exploited during penetration tests. Apparently, the security of traditional OA systems still cannot be overlooked.

Sum-up: The year of 2019 saw multiple remote code execution vulnerabilities that required no authentication to exploit, including the WebLogic XMLDecoder deserialization vulnerability, ThinkPHP remote code execution vulnerability, Apache Solr remote code execution vulnerability, and Atlassian Jira template injection vulnerability. These vulnerabilities were most favored by hacking groups that integrated the exploit code in a mature attack framework or a trojan to make it easier to take advantage of such vulnerabilities. Also, the time between vulnerability PoC announcement and mass exploitation is shortened, posing a greater challenge to security vendors' protection capability.

5.2 DDoS Threats

Key Findings:

1. **Maturity:** The technical maturity of attackers keeps growing, opening more possibilities than DDoS attacks for attackers to garner profits.
2. **Combination:** Of all DDoS attacks in 2019, 12.5% employed multiple vectors. This percentage was even higher among super-sized attacks (> 300 Gbps) to reach more than one-third. These

factors have posed a greater challenge to the performance of cleaning devices, the stability of cleaning lines, and the effectiveness of defense operations.

3. **Recidivists:** In 2019, a total of 1.3 million DDoS recidivists (involved in more than 20 attacks) were spotted, 7% of whom were responsible for 78% of attacks. Recidivist behavior deserves continuous attention.
4. **Gangs:** In 2019, a total of 60 DDoS gangs were detected, including 15 ones that contained more than 1000 attack sources. The largest gang, formidably, consisted of 88,000 attack sources. On average, 35,000 attack sources remained active every month. Therefore, we should keep vigilant on gang behavior and attack groups.
5. **IoT:** More and more IoT devices have been involved in DDoS attacks. In 2019, a single DDoS attack gang was found to contain 31% of IoT devices, among others. This is a phenomenon deserving continuous attention.
6. **Malware families:** IoT malware families launched an increasingly large proportion of attacks, as demonstrated by Gafgyt and Mirai. But, in general, there was no obvious change in DDoS signatures, attack targets, and C&C distribution.
7. **Location:** In China, Hong Kong overtook Zhejiang to become the biggest target of DDoS attacks, leaving Zhejiang in the second place, followed by Guangdong, Beijing, and Jiangsu.

5.2.1 Attack Trend

This section presents the DDoS attack trend in 2019 from perspectives of attack peak, attack count, and attack traffic.

Attack Peak Size

2019 saw 21,400 large-scale attacks peaking above 100 Gbps (according to data by November 2019), on a par with 2018 (22,000 by November 2018). Besides, super-sized attacks (> 300 Gbps) have increased year by year from an average of 30 per month in 2017 to 247 in 2018 and then to 262 in 2019. Arguably, it has become a normal thing for super-sized attacks to keep increasing in number.

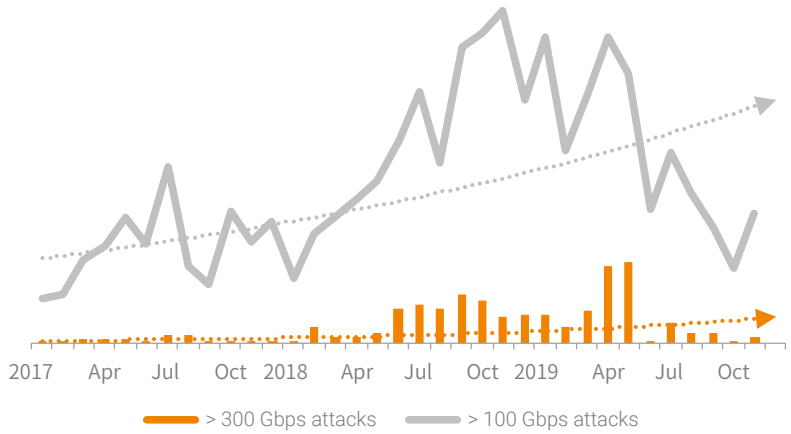


Figure 5-5 Monthly number of high-volume DDoS attacks in the last three years

Attack Counts and Attack Traffic

By November 2019, 167,400 DDoS attacks had been detected, generating a total of 436,800 TB traffic. On a year-on-year basis, the number of attacks increased 30.2%, but the total attack traffic decreased 26.4%, marking the first decline since 2017 when the total traffic doubled from the previous year.

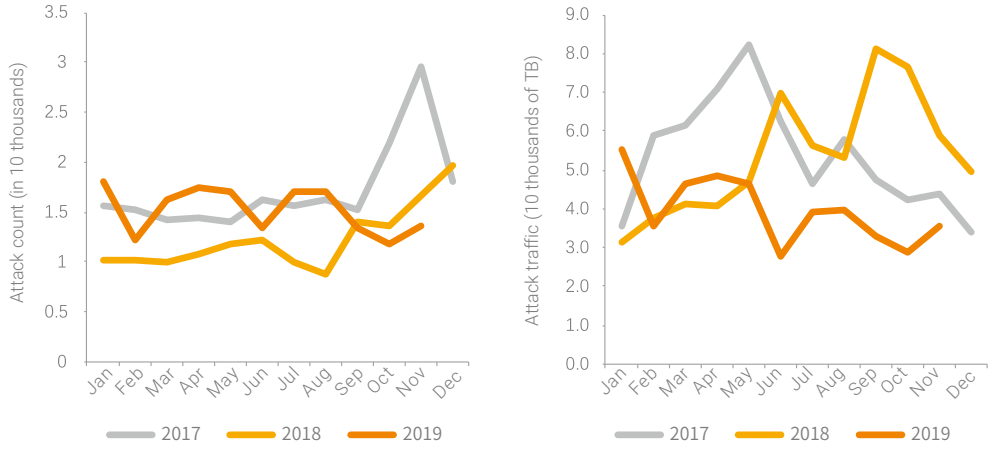


Figure 5-6 Attack count and attack traffic

5.2.2 Proportions of Different Attack Types

In 2019, most frequently seen attacks were UDP floods, SYN floods, and ACK floods, which together accounted for 82% of all DDoS attacks. By contrast, reflection attacks took up only 10%. Compared with 2018, reflection attacks rose slightly in number, but remained small in proportion.

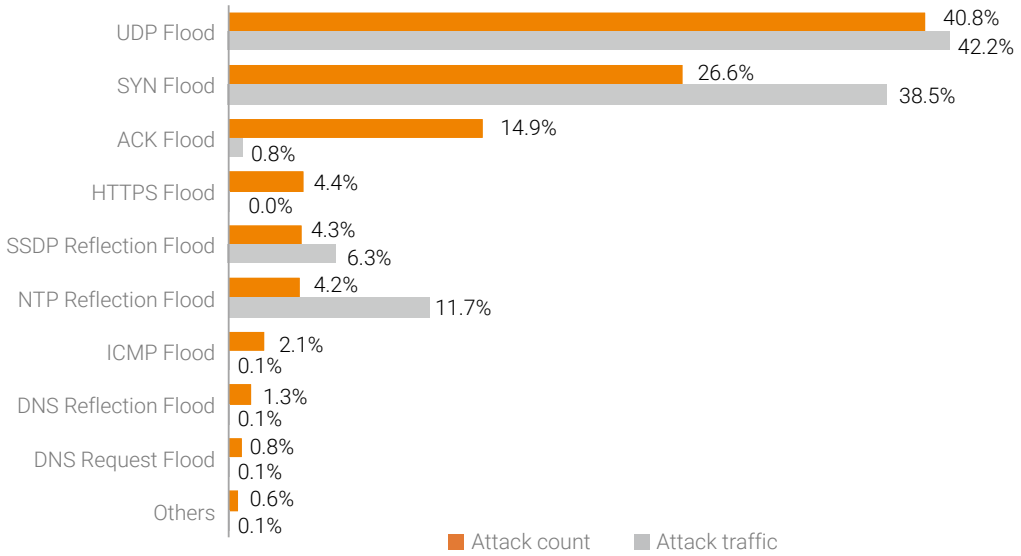


Figure 5-7 Proportions of different attack types by count and traffic

Source: NSFOCUS Threat Intelligence (NTI) and Cloud-based DDoS Protection Service (Cloud DPS)

Of all DDoS attacks, 12.5% used a combination of multiple attack methods. By flexibly combining several methods to adapt to different environments of target systems, attackers can initiate large amounts of traffic and exploit vulnerabilities in different protocols and systems, thus bringing their capabilities into full play. On the other side of the fence, defenders find it rather costly to effectively analyze, respond to, and mitigate such distributed attacks involving various protocols and leveraging various resources.

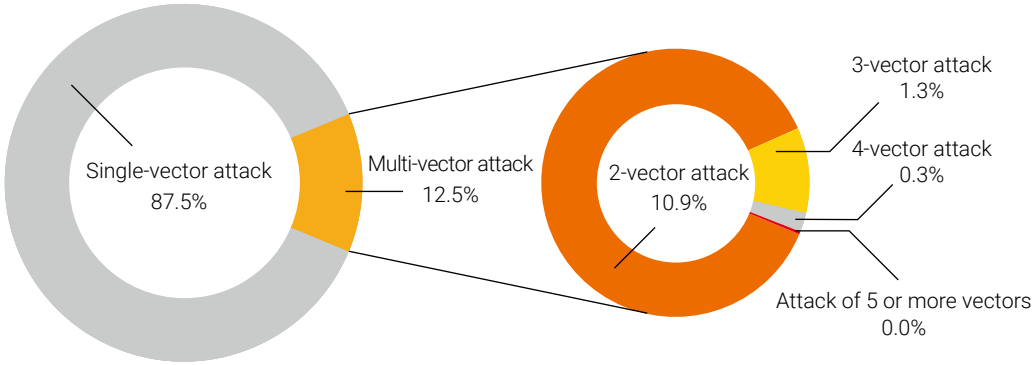


Figure 5-8 Distribution of multi-vector attacks

Source: NTI and Cloud DPS

The following figure shows the distribution of super-sized attacks (> 300 Gbps) in 2019. Obviously, SYN floods took the largest slice of the pie, followed by multi-vector attacks that stood at 32%. This posed a great challenge to the performance of cleaning devices, the stability of cleaning lines, and the effectiveness of defense operations.

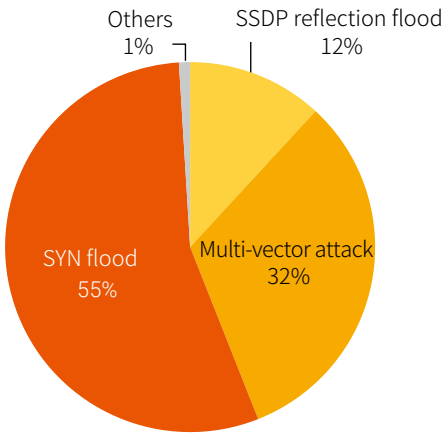


Figure 5-9 Distribution of super-sized attack types (> 300 Gbps)

5.2.3 Attack Gangs

In 2019, 7% of recidivists[1] were responsible for 78% of DDoS attacks. Obviously, recidivists are too menacing to overlook. Several groups of DDoS recidivists often work together to initiate attacks. Such groups are collectively referred to as an "IP gang". In 2019, a total of 60 DDoS gangs were detected, including 15 ones that contained more than 1000 attack sources. The largest gang, formidably, consisted of 88,000 attack sources. On average, 35,000 attack sources remained active every month. Therefore, we should keep vigilant on gang behavior and attack gangs. In this section, we will profile and analyze major attack gangs.

Largest Gang by the Number of Attack Sources

In 2019, the largest gang with most attack sources was also the most active one. This gang has 88,000 recidivists and its attack source device composition has a distinctive characteristic: According to asset intelligence from NTI, 31% of devices in this gang were IoT devices (28,000), 64% of which were routers (94% from MikroTik). This gang was active in the whole year, using 35,000 attack sources to hit 83 targets on average each month.

Figure 5-10 shows the monthly quantity trend of attack sources and attack targets of this gang. On average, 350,000 active attack sources launched attacks against 83 target each month. The quantity of attack sources of this gang fluctuated from month to month because some members left (the possible reason is that the system owner had removed the malware and fixed the security vulnerability exploited by the attack controller for system intrusion) while new members joined the gang (new systems were infected with malware and became botnet members).

1 In this report, "DDoS recidivists" refer to IP addresses that have persisted for a long time and launched more than 20 DDoS attacks.

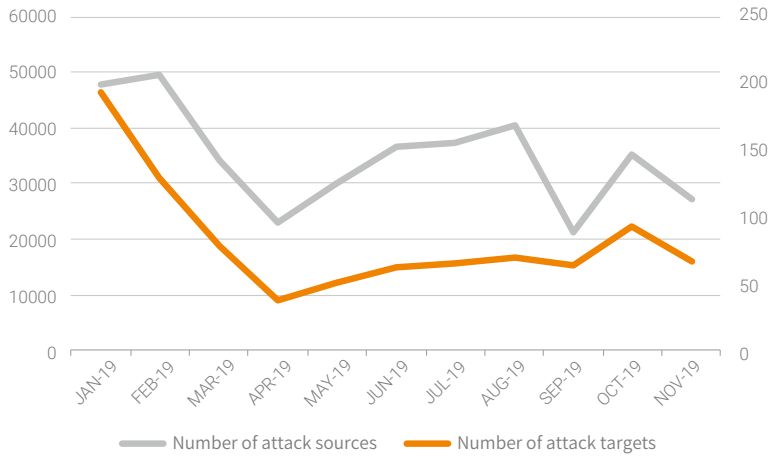


Figure 5-10 Monthly trend of attack sources and attack targets of the largest gang

Source: NTI and Cloud DPS

Figure 5-11 shows the activity distribution of the largest gang. The x-axis indicates the date (by day) and the y-axis indicates IP addresses of attack targets. A red spot indicates that this gang hits an IP address on a specific date. The size of a red spot represents the number of IP addresses of attack sources. The more intensive and greater the red spots are, the more active the gang is, that is, frequently performing DDoS attacks in a coordinated way. From the following figure, it can be seen that this gang stayed active throughout the year. Up to 11,300 attack sources in a gang hit one target at the same time in one day, a record high in a single day in 2019.

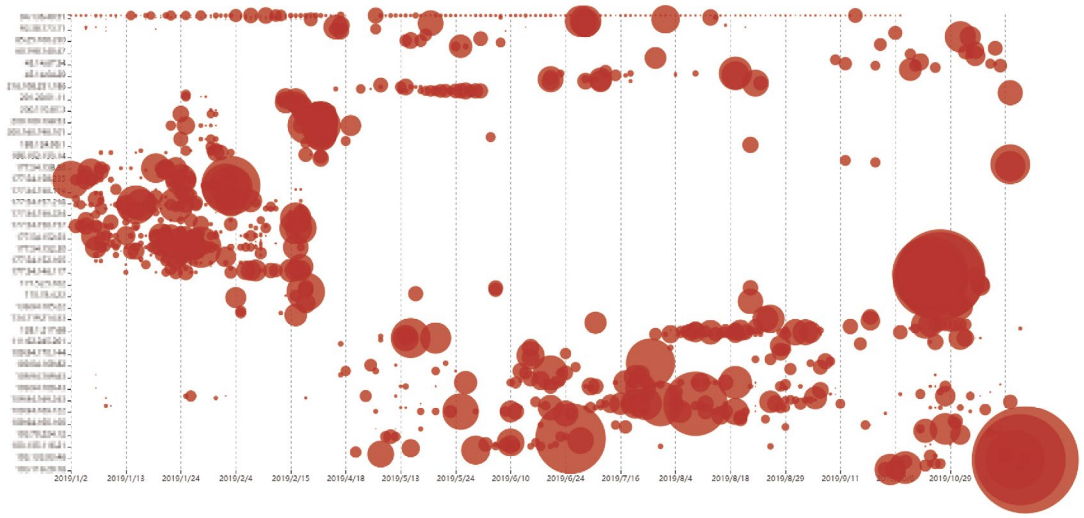


Figure 5-11 Activity distribution of the largest gang

Source: NTI and Cloud DPS

According to asset intelligence from NTI, IoT devices accounted for 31% of attack sources. Of all such IoT devices, 64% were routers and 94% of those routers were provided by MikroTik. In recent years, two vulnerabilities, CVE-2018-14847 and CVE-2019-3924, have been released for MikroTik. IoT devices are increasingly becoming favored zombies of hackers because they always stay connected, contain vulnerabilities that cannot be fixed in a short time, and are easily to break into and control.

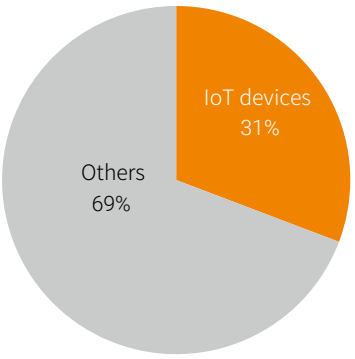


Figure 5-12 Attack type distribution of the largest gang

Source: NTI and Cloud DPS

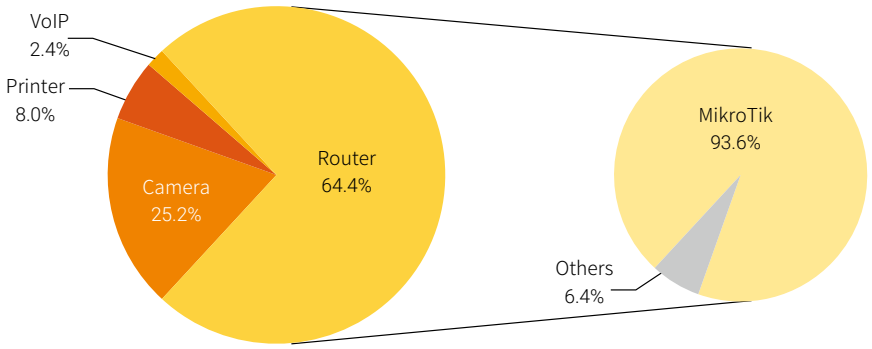


Figure 5-13 IoT device type distribution of the largest gang

Source: NSFOCUS ATM, Cloud DPS, and NTI

Second Largest Gang by the Number of Attack Sources

The second largest gang in terms of the number of attack sources generated the largest traffic. This gang had 23,000 recidivists and favored volumetric SYN flood attacks. According to historical attack records, 99.54% of recidivists had resorted to this kind of attack. This gang stayed active from January to October and was at its busiest in May.

Figure 5-14 shows the monthly quantity trend of attack sources and attack targets of this gang. We can see that this gang remained active from January to October, having more attack sources in January, April, May, and June. On average, 6000 active attack sources launched attacks against seven targets each month.

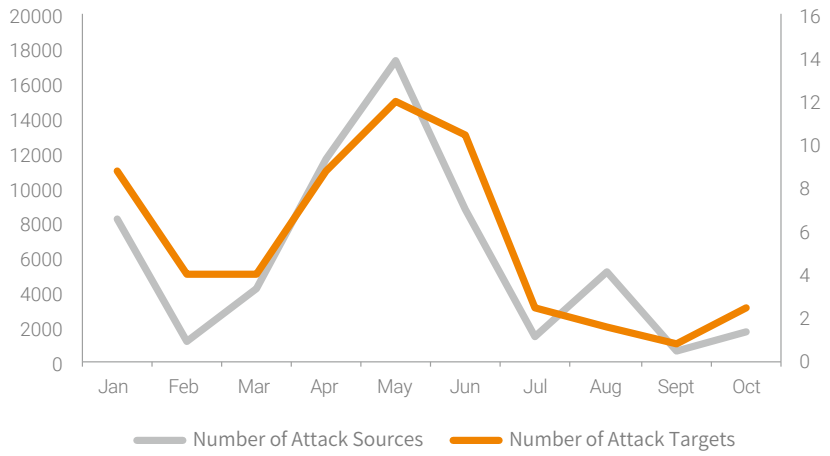


Figure 5-14 Monthly trend of attack sources and attack targets of the second largest gang

Source: NSFOCUS ATM, Cloud DPS, and NTI

Figure 5-15 shows the activity distribution of the second largest gang, with the x-axis indicating the date (by day) and the y-axis indicating IP addresses of attack targets. A red spot indicates that this gang hits an IP address on a specific date. The size of a red spot represents the number of members involved in attacks against this target. The more intensive and greater the red spots are on a specific date, the more active the gang is, that is, frequently performing DDoS attacks in a coordinated way. According to statistics, up to 8639 attack sources hit one target at the same time one day, the record high in a single day in 2019.

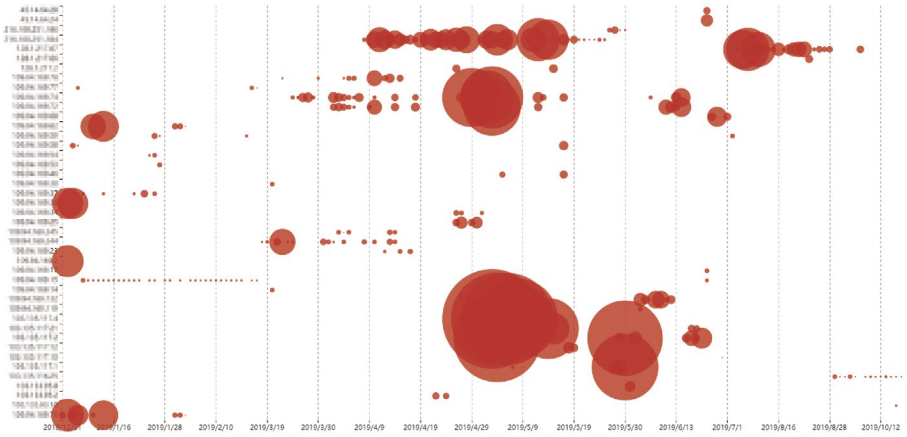


Figure 5-15 Activity distribution of the second largest gang

Source: NSFOCUS ATM, Cloud DPS, and NTI

Figure 5-16 shows the attack type distribution of the second largest gang. We can see that this gang mainly resorted to SYN flood attacks.

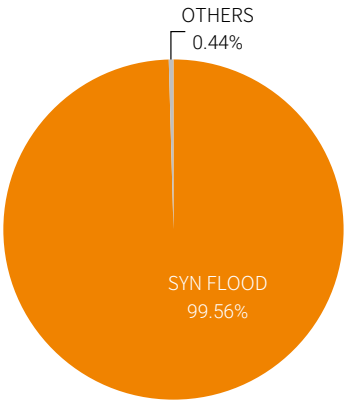


Figure 5-16 Attack type distribution of the second largest gang

Source: NSFOCUS ATM, Cloud DPS, and NTI

Peak traffic (Gbps) is a key indicator to measure a gang's attack ability and degree of maliciousness. Therefore, knowing the gang's upper capability limit is of great importance to defense planning. From the gang's peak traffic trend in 2019 shown in Figure 5-17, we can see that this gang frequently generated over 100 Gbps traffic, with superlarge traffic reaching over 300 Gbps on May 19 and 30 and

June 11 and even hitting 780 Gbps on August 15 in 2019. This fully explains that gang has robust attack capabilities and deserves our ongoing attention.

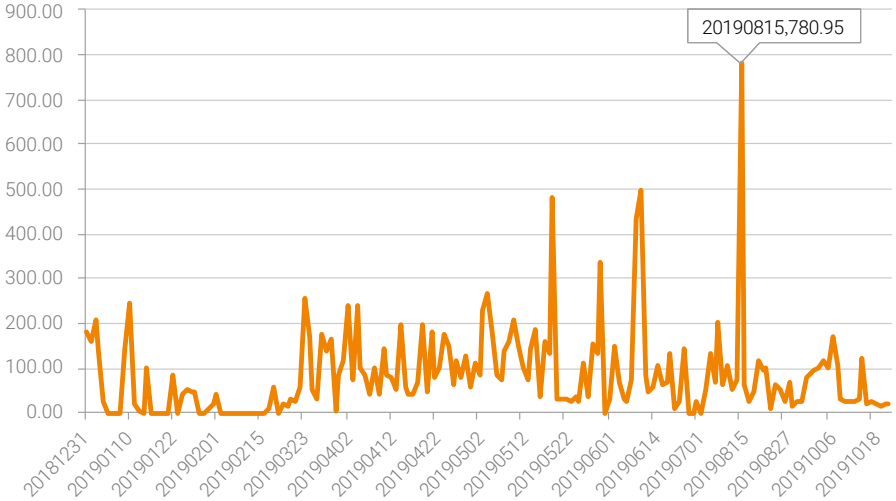


Figure 5-17 Peak traffic trend of the second largest attack source

Source: NSFOCUS ATM, Cloud DPS, and NTI

5.3 Cryptomining Threats

5.3.1 Cryptomining Traffic

Based on all sorts of security alert data from NSFOCUS Managed Security Service (MSS), we made a quantitative analysis of cryptomining activities and hosts in enterprises in 2019 and found that the cryptomining topicality is positively correlated with the cryptomining market trend.

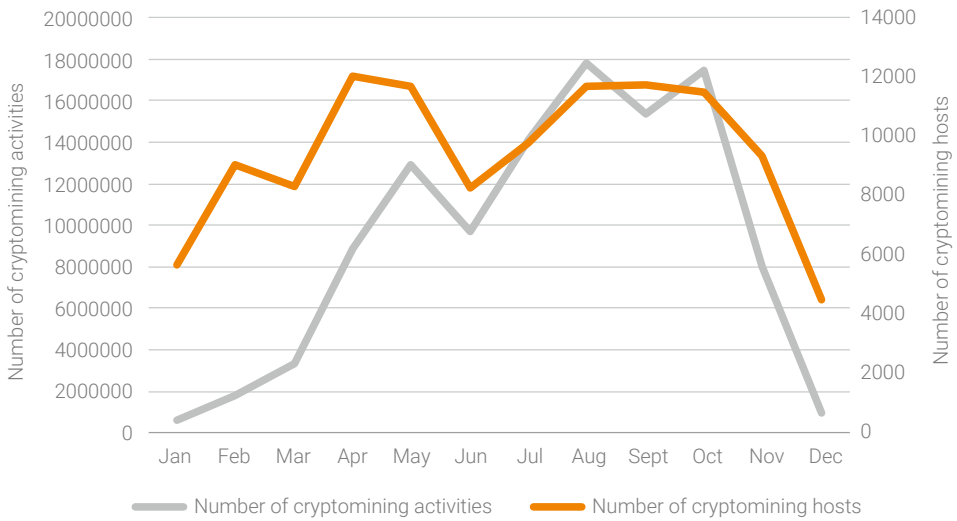


Figure 5-18 Trend of cryptomining activities within enterprises in 2019

JPMorgan Chase, a Wall Street bank tycoon, launched JPM coin [1] in February 2019. Avnet, a company listed on Fortune Global 500, becomes the third major technology company [2] that accepts Bitcoin for payment. All these signals encouraged hackers to feverishly carry out cyptojacking activities. In May, Binance, the world's biggest cryptocurrency exchange, had 7000 Bitcoins [3] stolen from its hot wallet. The poor security of cryptocurrency exchanges had provoked panic among investors, resulting in a big drop in the popularity of the cryptomining market. In July, Facebook released the Libra [4] whitepaper, sparking intense debates among regulatory bodies around the world. As the cryptocurrency community attracted worldwide attention, the Bitcoin price soared to $12,000 and cryptomining activities had reached their climax. In October, the trading of Bakkt [5] 's Bitcoin futures saw a slow start at launch which was touted as an important channel for capitals to go to the cryptocurrency market. Then came the closure of multiple American trading platforms. As the cryptomarket was badly hit once again, cryptocurrency activities were progressively reduced.

1 https://www.cnbc.com/video/2019/02/14/jp-morgan-rolling-out-its-own-cryptocurrency.html?&qsearchterm=JPM%20Coin
2 https://www.avnet.com/wps/portal/us/products/c/bitpay
3 https://www.zdnet.com/article/hackers-steal-41-million-from-cryptocurrency-exchange-binance
4 https://developers.libra.org/
5 https://www.bakkt.com/index

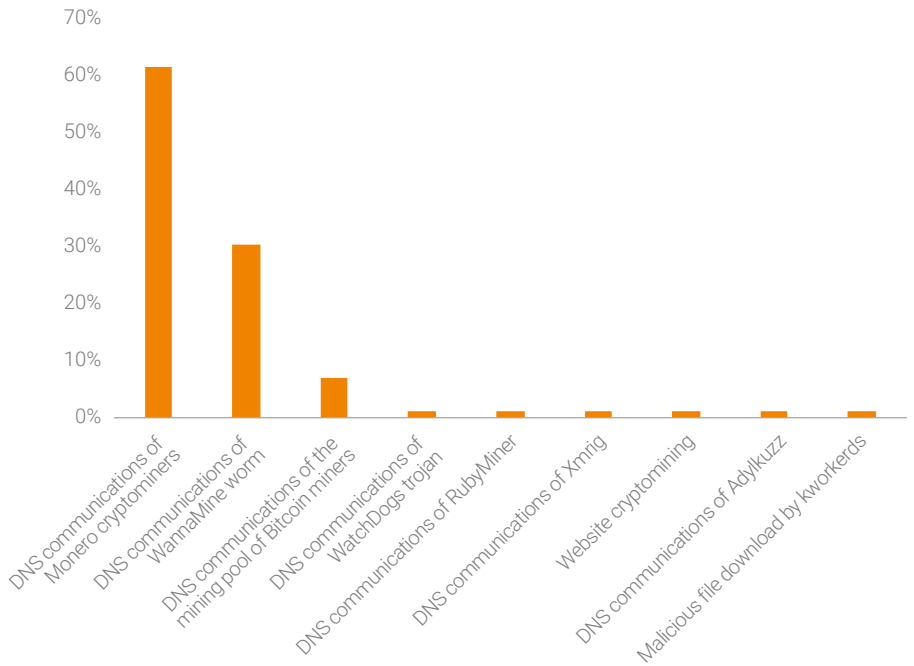


Figure 5-19 Distribution of cryptomining behaviors

Monero is an untraceable anonymous cryptocurrency that obfuscates sending and receiving addresses as well as transacted amounts. Its anonymity makes it the most popular cryptocurrency circulating on the dark web market. We made a further analysis of specific cryptomining activities throughout 2019 as shown in Figure 5-20 and found that 60% of cryptomining behaviors were performed by Monero miners requesting the domain name of the mining pool. The WannaMine worm, with the second largest proportion of cryptomining behaviors, had a new variant WannaMine4.0, at the beginning of 2019, which still uses the original attack means, i.e., exploiting the EternelBlue vulnerability to infect a large number of intranet hosts for malicious cryptomining.

Figure 5-20 shows the distribution of cryptomining victims by sector. It can be seen that small and medium-sized enterprises were favorite targets of cryptominers, making up 80% of cryptomining victims. For these malicious activities, attackers usually intruded into and controlled cryptomining hosts by scanning for common vulnerabilities in batches. This demonstrates that maintenance staff in those enterprises lack basic security awareness.

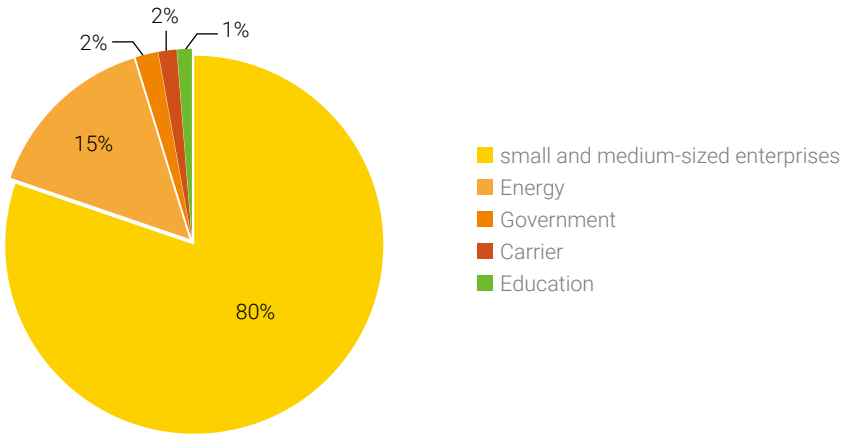


Figure 5-20 Distribution of cryptomining victims by sector

Besides ports 80 and 443, attackers tended to use rare ports to connect to the cryptomining pool. As shown in Figure 5-21, port 3333 was the most favored port of cryptominers. According to the distribution of cryptomining activities by port range, ports in the range of 3000–3999 were used most frequently, involving 43% of all ports used by cryptomininers. Ports ranging from 5000 to 5999 came second, with a percentage of 13% of the total. As specific cryptomining ports and cryptomining pool addresses are part of behavior patterns of attackers of malicious cryptomining, enterprises can prevent this kind of activities by blocking cryptomining ports.

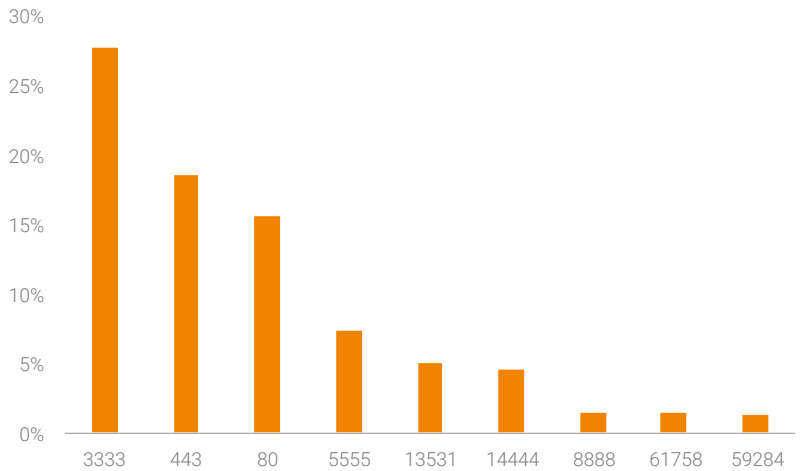


Figure 5-21 Distribution of cryptomining activities by commonly used port

5.3.2 Website Cryptomining

Website cryptomining refers to a process of malicious cryptomining implemented via automatic JavaScript execution to consume considerable computer resources without the knowledge of a user tricked into accessing a website on which such JavaScript is planted. Instead of planting a cryptomining trojan on a host, an attacker of this type can reduce a user's host to a cryptomining host simply by tricking the user into accessing a malicious page.

To measure the impact of such attacks, we analyzed the source code of top 1 million websites by Alex Rank and found 2567 cryptomining domain names that mainly mined Monero with heaviest use of the Coinhive cryptomining script.

As shown in Figure 5-22, cryptomining websites were scattered in different Alexa ranking intervals, with 330 included in top 100,000 websites. Cryptomining gains are directly associated with website visits. That is to say, a website with more visits is ranked better and rakes in higher cryptomining profits.

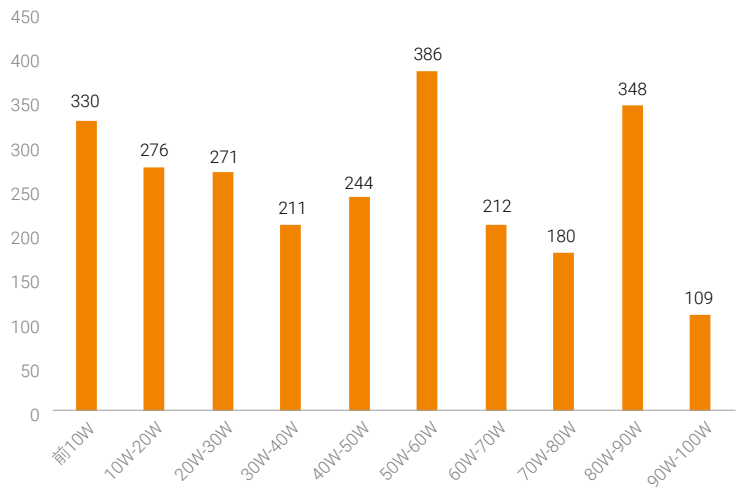


Figure 5-22 Distribution of cryptomining websites scattered in top websites by Alexa Rank

According to the distribution of cryptmining website types shown in Figure 5-23, we can see that cryptoming websites for business and entertainment dominated with a percentage of 22% and 19% respectively. This is because this kind of websites have larger access traffic. In addition, some website owners proactively embed cryptomining scripts into personal websites or blogs to increase their own

cryptomining gains by using visitors' computer resources. Such practice, however, greatly affects user experience.

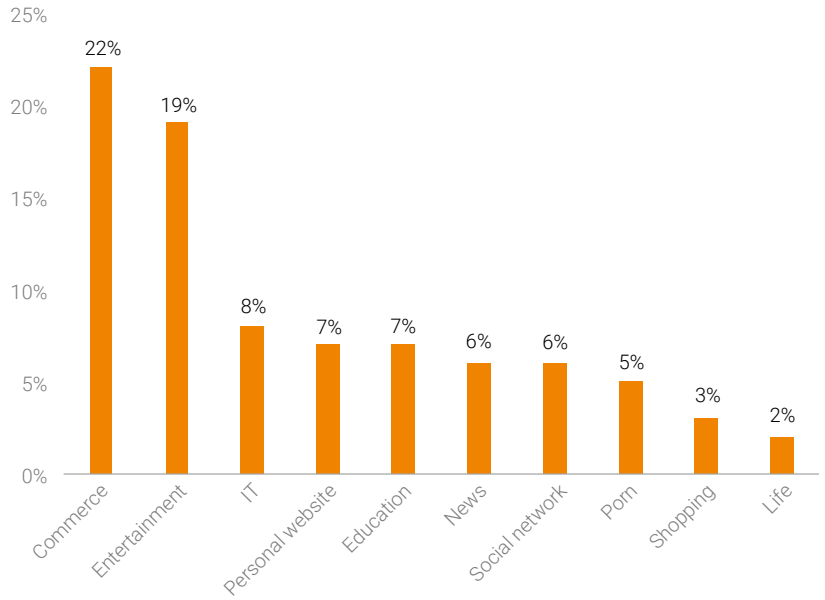


Figure 5-23 Distribution of cryptmining website types

5.3.3 Cryptomining Botnets

By aggregating attack behaviors performed by attack sources that used Telnet extensively for intrusion, we made a correlative analysis of the related list of weak passwords for cracking and malicious samples and identified a botnet that mined Monero. This botnet first broke into a host by cracking a weak password, so as to plant an RSA public key or botnet to take control of the host. Then it used a downloader to download a Monero cryptomining virus to execute the script matching the host type, thereby implementing malicious cryptomining and reaping benefits using the controlled network resources.

Figure 5-24 shows the overall situation of the cryptomining botnet. According to a rough estimate, this botnet controlled tens of thousands of zombies and was found most active in July in which the number of zombies topped at nearly 600 in a single day in 2019. Most zombies resided in China (2119) and the

USA (1335). A total of 6681 zombies opened port 22, making up 65% of the total. According to known asset intelligence, 12% of all zombies were identified as IoT devices, with routers and cameras as dominant players. As for weak passwords for cracking, this botnet used nproc-nproc most frequently. Though related samples could not be downloaded from the sample server currently, we observed that there was still a modest increase in activities of this botnet.

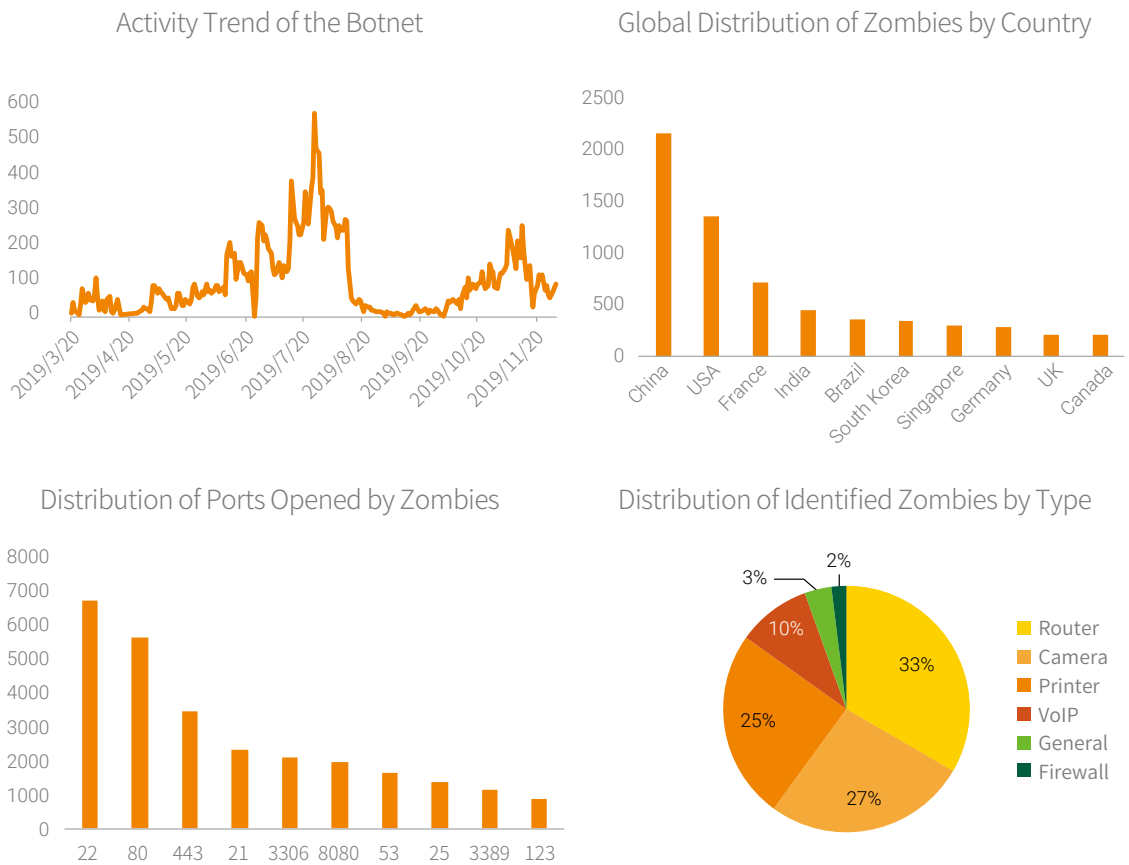


Figure 5-24 Overview of Cryptomining Botnet

For the complete analysis of this botnet, refer to a post [1]on NSFOCUS Research Communications.

1 The Idea of Making Money Through Blockchains Also Occurring to Hacking Groups, https://mp.weixin.qq.com/s/lzqWgX0bHXfOiBelovV3bA

6

Malware

6.1 Ransomware

In 2019, ransomware was still a major type of threats that haunted people around the world. The most prominent families were GlobeImposter, GandCrab, and WannaCry, which were extremely active and had far more variants than others. According to NSFOCUS Security Labs' observation, the number of ransomware families and variants increased sharply in four months from May to August 2019, which was somewhat attributable to the soaring prices of major cryptocurrency types. These families used diverse compromise methods to attack a wide variety of sectors, posing a severe threat to organizations' and individuals' data. Through ongoing monitoring, NSFOCUS Security Labs finds that the following trends of ransomware took shape in 2019:

1. Victimizing targets across a wide range of sectors

In 2019, ransomware victims were distributed in various industries, including finance (23.8%), telecom (16.6%), governments (14.3%), real estate, chemicals, tobacco, healthcare, and IT. Obviously, ransomware attackers were most interested in finance, telecom, and real estate, all of which are lucrative sectors and capable of paying high amounts of ransom.

2. Enabling hackers to rake in high returns

Ransomware enables hackers to make a killing. Take the GandCrab family as an example. First spotted in 2018, the ransomware stopped operation in June 2019 upon the operator's declaration. According to the organization, in only 18 months, they raked in up to USD 2 billion of ransom and, abominably, legalized this income.

3. Moving faster towards industrialization

Ransomware as a Service (RaaS) is maturing, enabling cyber criminals to do evil at an increasingly low cost.

Moreover, inspired by their predecessors who have been successful in getting rich quick, more people are attracted to this lucrative business, giving birth to more diversified ransomware. The brazen behavior of the organization behind GandCrab is not only a blatant provocation to cybersecurity law enforcement and professionals but also an effective move to invite more copycats to this line of trade.

Sodinokibi, another ransomware family, bears resemblance to GandCrab in many an aspect and is so regarded as the inheritor of the latter. After a successful ransomware attack, a ransom note will be displayed, instructing users to access specified websites. These websites provide multiple channels for purchasing Bitcoins as well as a 24/7 customer support platform for both parties to negotiate the ransom amount, exhibiting a high level of industrialization.

4. Boasting a variety of compromise and spreading methods

In 2019, ransomware families were found to use a variety of methods to spread themselves, including weak password cracking, remote exploit, phishing, URL redirection, and bank trojans. Specifically, EternalBlue stood out from other remote exploits. Vulnerabilities in such cross-platform components as Adobe Flash, WebLogic, and Confluence were also targeted, but related exploits were not so popular as EternalBlue because of the limited usage of these components. Moreover, some ransomware families were spread via notorious bank trojans like Emotet and TrickBot for targeted ransom demands.

In view of the diverse compromise methods of ransomware, IT managers should back up data more frequently in a regular manner besides properly maintaining and upgrading systems.

6.2 Cryptojacking Malware

In 2019, the pickup in cryptocurrency prices led to an increase in the number of cryptojacking malware families. Of all these families, Monero mining trojans still took a dominant place. EternalBlue and weak password cracking were the major methods for ransomware families to compromise large enterprises in financial and telecom sectors and spread themselves. At the same time, to defeat detection devices, cryptojacking malware families have been constantly upgraded to evolve into more variants that feature better stealth and a modular design.

1. Monero mining remaining a much-pursued activity

According to statistics, the most commonly used mining pool was pool.minexmr.com (46%) in 2019. Most mining pools support Monero, an indirect indicator of the strong presence of Monero mining malware. Their IP addresses revealed that these mining pools were mostly located in North America and Europe, with only a small proportion in East Asia due to cryptocurrency policies of Chinese, Japanese, and South Korean governments. Monero is anonymous, fungible, and censorship resistant, making itself a coveted target for cryptojackers intending to hide their traces from detection devices.

2. Modular design

Cryptojacking malware is coming to maturity. Some families are showing an inclination of using a modular design, allowing flexible configuration of different payloads for different campaigns.

A typical example of modularized cryptojackers is WannaMine, which consists of scanning, exploit, download, persistence, and other modules. As a cryptojacking family, WannaMine, unexpectedly in 2019, acted out of normal behavior to spread DDoS payloads, indicating that different types of malware may cross boundaries when it comes to money.

3. Anonymity

Untraceability is becoming increasingly necessary for cryptojacking malware, which explains why fileless attacks are gaining popularity. Cryptojackers using this technique are mainly built on PowerShell, leveraging scheduled tasks to reside in systems in an unnoticeable manner.

Moreover, cryptojacking malware tries to juggle things at the levels of system files and drivers. In September 2019, NSFOCUS detected a Monero cryptojacking attack launched by exploiting a vulnerability in Redis. The malicious payload SkidMap (dubbed by McAfee and Trend Micro) used in this attack would replace binaries of multiple common Linux commands and load a malicious driver to avoid detection. This type of attacks, which combines a backdoor and rootkit, further improves the anonymity of malware and so is more difficult to detect.

4. Myriads of compromise methods

In 2019, cryptojacking malware usually attacked targets by means of remote exploits. EternalBlue and

other exploits targeting vulnerabilities in web frameworks (Hadoop Yarn, Apache Struts 2, Confluence, WebLogic, and Jenkins) were most frequently used by cryptojackers to compromise targets and spread themselves. Besides, weak password cracking against Oracle, MySQL, and other databases was also a common attack method.

In terms of the target sectors, finance and telecom were two favorite ones for cryptojacking malware. These sectors usually have a great number of high-performance servers and personal computers deployed to meet their business needs. More often than not, these servers are not properly maintained as expected, making it possible for cryptojackers to gain persistence.

For these reasons, IT managers and operators should upgrade and patch systems in time and configure strong passwords for login to devices to protect enterprises and individuals from being compromised by cryptojackers.

6.3 Malware Threats from Mobile Platforms

Nowadays, smartphones are ubiquitous. Android, as a widely used mobile operating system, is vulnerable to an increasing large number of malware families owing to its openness and privilege issues. Such malware can even be spread via legal channels, including Google Store.

Generally, the evolution of mobile platform threats shares great similarities with that of PC threats. In 2019, ad apps still dominated the list of malware threatening the security of Android users. Potentially dangerous software requiring sensitive operations also made up a large proportion. High-risk threats, such as spyware, bank trojans, and ransomware, were small in number, but most of them had been around for some time and some even for years. Agent programs launching attacks via remote code execution, thanks to the inherent nature of Android, were another type of mobile threats at the top of the list.

1. Compromise and spreading method

As usual, active malware on mobile platforms in 2019 was mainly distributed via third-party markets and illegitimate links. Although this type of malware, as a whole, made not much headway technically,

bank trojans and ransomware became more skilled in social engineering and could launch attacks by means of highly deceptive content. When it comes to the grey industry, 2019 saw more and more apps bundled with malicious functions or modules intentionally by developers or stealthily by evil-minded people.

With the development of mobile operating systems and markets, malicious Android applications are now easier to remove. However, for ordinary Android users with little security awareness, these malicious applications can still significantly affect the user experience or even cause financial losses. Android users should remember to keep their systems up to date and obtain content from legitimate channels to avoid being attacked and leveraged by cyber criminals.

2. Adware

In 2019, Android adware could be classified into the following types from the aspect of the delivery method:

Bundled adware. When developing such adware, the writer decompresses a popular, legitimate app and then adds an ad module to it before compressing and uploading the tampered package to third-party app markets. An example of this type of adware is Ewind.

Disguised adware. Adware has an icon and name looking identical or similar to a popular app and is available on third-party app markets. MobiDash is a typical example of this type of adware.

Adware in the form of the software development kit (SDK). Some adware developers have acquired the legal status and do business by pushing their own adware in the form of SDKs to partners. Applications using these SDKs will be included in the ad push network to have their ads displayed, thus garnering profits. AirPush is such a type of adware.

Though different in the delivery method, all these types of adware could cause bad experience to Android users. Most of such software has a delay mechanism by which ads are not pushed until hours or even days after the software is installed, adding to the difficulty of identifying it by users and regulators.

3. Bank trojans

In 2019, bank trojans like Wroba, Svpeng, and Asacub were extremely active around the world.

Wroba is a long-lived bank trojan targeting South Korean users. Looking like common bank applications (Hana Financial Group, Lotte Co., Ltd., and so on), Wroba is delivered via phishing websites or links. This trojan is mainly used for stealing app information, call records, short message service (SMS) contents, and other information. Specifically, it forges web pages to collect users' bank account information and then sends such information to a specified C&C server.

Svpeng is a bank trojan mainly targeting Russian users. Usually disguised as an application like Flash Player or a popular game, the trojan is distributed via application markets. It is mainly used for espionage purposes, including collecting SMS, call, and keystroke records of devices, sending text messages, and obtaining administrative privileges to gain persistence. In addition, with a forged credit card page, the malware can collect users' credit card information.

It is worth noting that some Svpeng variants have the ransomware feature, enabling the malware to demand ransom from users while collecting user information.

Asacub is also a long-lived bank trojan targeting Russian users. It has evolved into a full-featured remote control trojan from a simple secret theft tool. The initial version of Asacub features a small size and a simple function of stealing users' SMS contents. The mobile banking evolution of Asacub includes features that enable the trojan to display a phishing page for a banking application, execute command-line instructions, and capture screens. By hijacking users' SMS contents, Asacub can leverage social engineering to achieve fast spreading.

4. Ransomware

Some variants of the banking trojan Svpeng come with the ransomware feature, which is achieved by locking users' screens, the oldest practice of Android ransomware. These variants had the most samples detected in 2019 among all ransomware families. With US Android users as the major targets, the variant disguises itself as an application offering adult content. During running, it uses a high-privileged window to freeze the screen and disable all buttons except the power button. Besides, it

accuses users of viewing illegal content on their smartphones and uses it as an excuse to demand users to pay ransom.

Fortunately, ransomware families are less original in their delivery method. Android users can walk around them as long as they avoid downloading applications from unofficial channels.

5. Cryptojacking malware

Some Android applications engage in cryptojacking activities without users' knowledge by including a cryptomining module.

Usually, cryptomining can be achieved via JavaScript scripts or a shared object (SO).

Android applications embedded with JavaScript cryptomining scripts are massive in quantity. They include not only malicious applications but also legitimate ones. These applications seem to prefer Android TV boxes to smartphones. This is because TV boxes have poor application governance and applications on them usually run continuously for hours, providing a good chance for hackers to garner more profits by means of cryptojacking.

Compared with JavaScript scripts, SOs are characterized by more efficient cryptomining and larger file sizes. The latter characteristic makes it difficult to spread SOs by means of bundling. Common SO cryptomining modules include NeoNeonMiner and MinerGate, built on mainstream architectures such as x86/x64, ARM, and MIPS.

7

IoT Threats

Finding 1: In 2019, over 30 types of IoT vulnerability exploits were captured, most of which targeted remote command execution vulnerabilities. Though hundreds of to thousands of IoT vulnerabilities are unveiled each year, only a few can exert an extensive impact. Attackers were keen on targeting devices (routers and video surveillance devices) exposed in large quantities, in a bid to broaden their influence.

Finding 2: IoT devices, especially cameras and routers, were major targets of Telnet weak password cracking attacks.

Finding 3: Since security researchers from Baidu disclosed that the Web Services Dynamic Discovery (WSD) protocol could be exploited for DDoS reflection attacks, there has been a notable increase in reflection attack events based on this protocol in the latter half of 2019. Since mid-August, WSD reflection attacks captured by us have been on the rise. Worse still, September has witnessed a sharp increase in such attacks. All parties concerned, including security vendors, service providers, and telecom carriers, should pay due attention to this type of threats.

Finding 4: Approximately 2.28 million IoT devices (port 1900) worldwide had the UPnP/SSDP service publicly accessible and were thus at risk of being exploited to launch DDoS attacks, an decrease of 22% from 2018.The UPnP port mapping service, exposed on about 390,000 IoT devices, was likely to be abused as a proxy or render intranet services accessible on the extranet.

7.1 IoT-related Exploits

7.1.1 IoT-related Malware

In the past few years, the IoT has gained momentum for rapid development, giving rise to an increasing variety of IoT devices, including processors, routers, cameras, and smart devices. These devices have insufficient safeguards. Successful exploitation of their vulnerabilities could lead to escalated system privileges. By analyzing attack alerts generated by intrusion prevention systems (IPSs), we can find out which vulnerabilities were most favored by hackers and how many times they were involved in actual attacks in 2019.

Table 7-1 IoT device exploits

Vulnerability	Number of Alerts
Netcore/Netis Router Backdoor	5,013,213
Dahua Surveillance Device Unauthorized Access Vulnerability	169,930
D-Link DSL-2750B Arbitrary Command Execution Vulnerability	140,471
TP-Link Wireless Router HTTP/TFTP Backdoor Vulnerability	55,051
Schneider Pelco Sarix Enhanced Camera Command Execution Vulnerability	29,418
Schneider Pelco Sarix Pro Camera session.cgi Buffer Overflow Vulnerability	28,472
Huawei HG532 Router Remote Command Execution Vulnerability (CVE-2017-17215)	14,730
D-Link Router User-Agent Backdoor Vulnerability	9608
Motorola Wireless Router WR850G Authentication Bypass Vulnerability	4208

Vulnerabilities in IoT devices stem from web applications, systems, and protocols. As for web applications, users usually use default settings and weak passwords, exposing devices to SQL injection and XSS threats. At the system level, as far as cameras are concerned, the read-only memory (ROM) usually uses such file systems as SquashFS, JFFS2, and UBIFS, which contain some vulnerabilities. Whether the firmware is upgraded in time depends on the importance attached by device vendors on the one side and users' willingness to promptly upgrade it on the other side. Finally, there is a broad variety of application protocols. Cameras alone use the Universal Plug and Play (UPnP), Real-Time Streaming Protocol (RTSP), and standards and specifications from the Open Network Video Interface Forum (ONVIF). If these protocols contain unauthorized access vulnerabilities, there is a good chance of cameras being attacked by hackers.

7.1.2 IoT-related Vulnerabilities Exploited

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

Over 30 types of IoT vulnerability exploits were captured, most of which targeted remote command execution vulnerabilities. Arguably, from the perspective of global IoT threats, though hundreds of to thousands of IoT vulnerabilities are unveiled each year, only a few can exert an extensive impact. We counted all logs generated one day for a source IP addresses as one attack event. Upon deduplication of attack IP addresses, we got top 10 IoT vulnerabilities listed in the descending order of exploitation

quantity in Table 7-2. It can be seen that attackers' vulnerability exploits mainly targeted routers and video surveillance devices, which fits in with the fact that routers and video surveillance devices were major IoT devices exposed on the Internet. Evidently, attackers prefer to hit devices exposed in large quantities to extend their influence. The proof of concept (PoC) of most of these vulnerabilities can be found in the Exploit Database and those beyond this database are available on GitHub. Those publicly available PoCs have substantially reduced attackers' cost of crafting attack payloads.

Table 7-2 Top 10 IoT vulnerabilities by exploitation quantity

Exploit-DB No.	Vulnerability Exposure Year	CVE ID	Vulnerability Description
43414	2017	CVE-2017-17215	Huawei Router HG532 - Arbitrary Command Execution
37169	2014	CVE-2014-8361	Realtek SDK - Miniigd UPnP SOAP Command Execution
40740	2016	CVE-2016-10372	Eir D1000 Wireless Router - WAN Side Remote Command Injection
N/A	2018	N/A	Shenzhen TVT Digital Technology Co. Ltd & OEM {DVR/NVR/IPC} API RCE
43387	2014	N/A	Netcore / Netis Routers - UDP Backdoor Access
31683	2014	N/A	Linksys E-series - Remote Code Execution
37171	2015	CVE-2015-2051	D-Link Devices - HNAP SOAPAction-Header Command Execution
41471	2017	N/A	MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution
43055	2017	N/A	Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution
44760	2018	N/A	D-Link DSL-2750B - OS Command Injection

After statistics deduplication, we analyzed the global distribution of source IP addresses. As shown in Figure 7-1, China was home to most malicious IP addresses, about one order of magnitude higher than other countries following it such as Brazil, the USA, and Russia. In China, up to 20,000 IP addresses initiated exploit behaviors, 85% of which resided in Taiwan. Of those attack behaviors, nearly 90% targeted the same UPnP vulnerability (CVE-2017-17215).

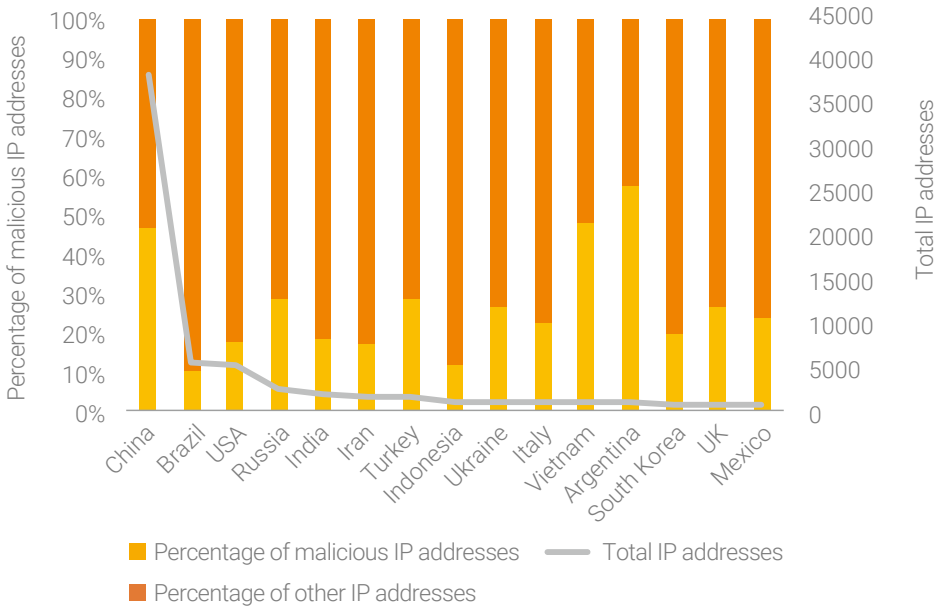


Figure 7-1 Global distribution of source IP addresses targeting IoT devices

Figure 7-2 shows the global distribution of IP addresses of servers for download of exploit payload samples. Obviously, the USA had the most sample download servers, with a percentage of 15.9%.

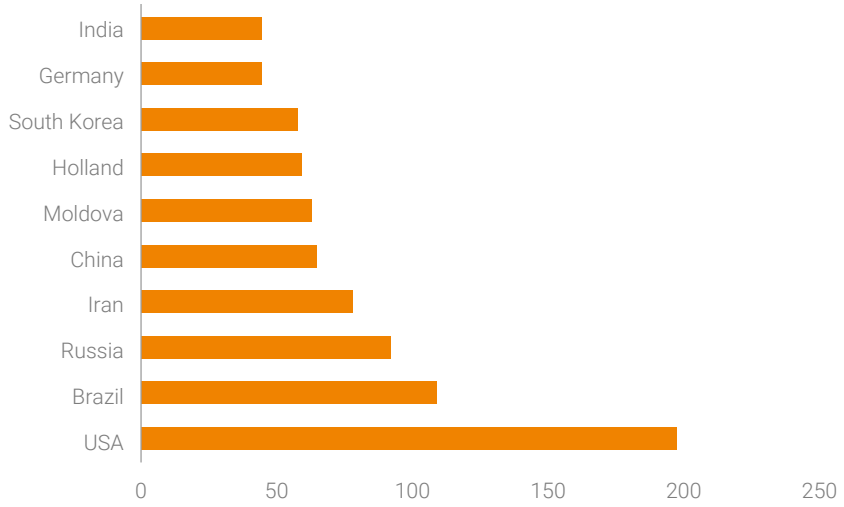


Figure 7-2 Top 10 countries with the most IP address of IoT exploit sample download servers

7.2 Threats Against IoT Protocols

In this section, we analyzed threats against three major protocols.

7.2.1 Threats Against Telnet

According to data from NSFOCUS's threat hunting system, Telnet (available on port 23), targeted by a total of 120,000 attack sources, was the IoT protocol most favored by attackers[1] . Figure 7-3 shows the activity trend of Telnet attack sources from March to October in 2019. We can see that the number of Telnet-based attacks increased month by month from March to August, with August seeing the most attack sources (over 60,000) that carried out more than 50,000 weak password detection activities. In addition, June witnessed the most sample download activities (more than 40,000). Overall, attack sources were on the decline in the latter half of 2019.

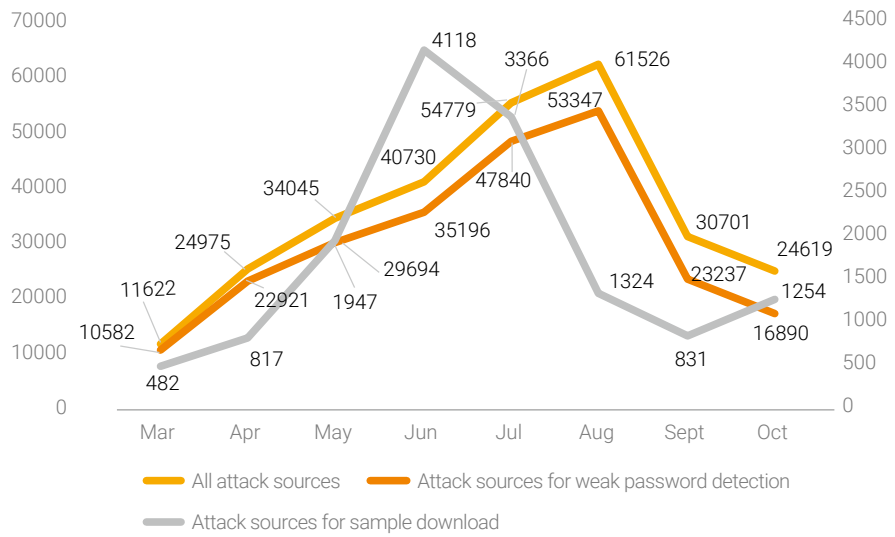


Figure 7-3 Activity trend of Telnet attack sources

We analyzed attack sources from the geographical perspective and got top 10 countries with the most attack sources, as shown in Figure 7-4. Apparently, China and the USA took top two spots.

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

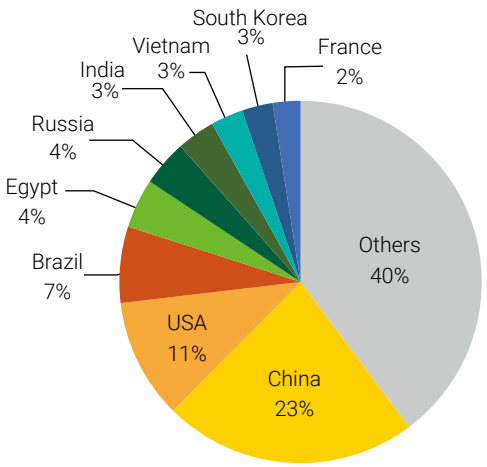


Figure 7-4 Global distribution of Telnet attack sources

By correlating with asset intelligence data from NTI, we found that IoT devices accounted for 29% of attack sources, with routers (47%) and video surveillance devices (42%) as dominant players. See Figure 7-5. Arguably, the two kind of devices were most easily exploitable IoT devices.

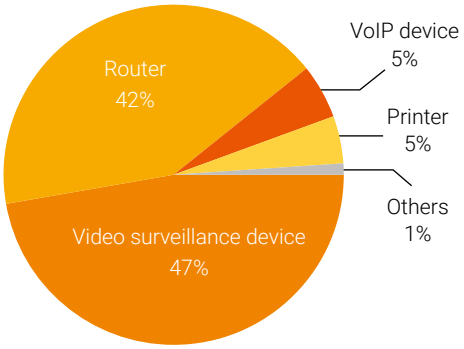


Figure 7-5 Distribution of Telnet attack sources by type

Weak password cracking is the major means resorted by attackers to target Telnet. We made an analysis of weak password exploitation and found that many IoT devices were compromised after suffering weak password cracking. Table 7.3 lists top 10 weak passwords for cracking. Of those passwords, root-vizxv was cracked for a direct login to the background of security surveillance devices from Dahua; root-t0talc0ntr0l4! was the default access credential of smart home devices of Control4;

root-taZz@23495859 was one of the weak password most frequently used by Asher, a Mirai variant, to infect routers.

Table 7-3 Top 10 Telnet-based weak passwords for cracking

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

7.2.2 Threats Against WS-Discovery

WSD is a multicast discovery protocol to locate services on a local area network (LAN). However, due to device vendors' design flaw in the implementation, when a normal IP address sends a service discovery packet, devices will also respond to the request. If exposed on the Internet, these devices will be possibly exploited for DDoS reflection attacks. In February 2019, security researchers [1] from Baidu published an article [2] about WSD reflection attacks. This is the first report we have read about such attacks. In a post [3], ZDNet mentioned that WSD reflection attacks were first reported in May, and in August, many organizations began to use this protocol to launch DDoS attacks. According to Akamai [4],

1 For the involvement of ONVIF-based IoT devices in DDoS reflection attacks, visit https://www.freebuf.com/articles/system/196186.html

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

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

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

one of its customers in the gaming industry suffered a WSD reflection attack weighing in at 35 Gbps at peak bandwidth.

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

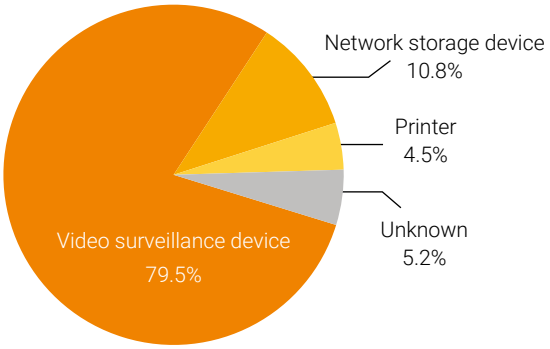


Figure 7-6 Distribution of types of devices with the WS-Discovery service publicly available

Figure 7-7 shows the global distribution of devices with the WS-Discovery service publicly available. We can see that China, Vietnam, Brazil, the USA, and South Korea saw the most devices with this service publicly available.

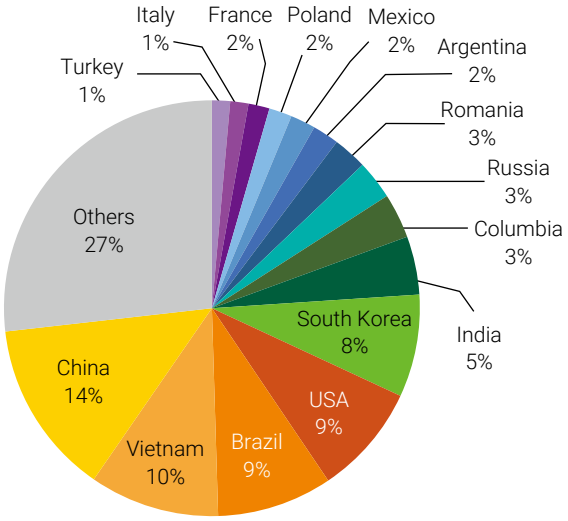


Figure 7-7 Global distribution of devices with the WS-Discovery service publicly available

We analyzed attack events captured by NSFOCUS's threat hunting system. Here all events about one IP address in one day add up to an attack event. Figure 7-8 shows the daily number of attack events. At a glance, WSD reflection attack incidents fluctuated all the time, but had been on the rise generally since mid-August, especially in September. This indicates that WSD reflection attacks have been gradually adopted as a regular weapon of DDoS attacks, to which all parties concerned, including security vendors, service providers, and telecom operators, should pay due attention.

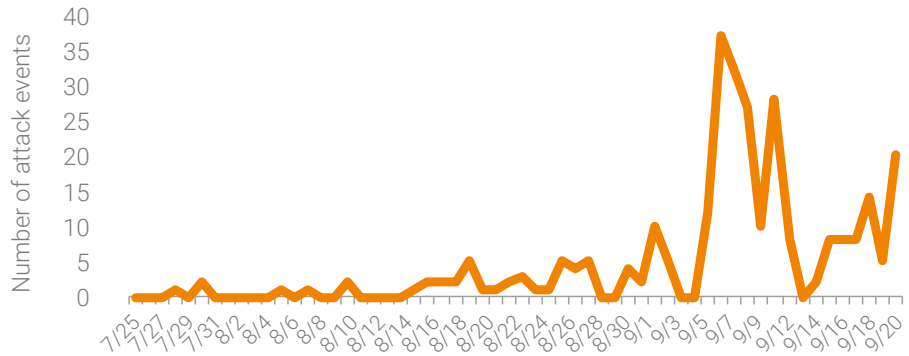


Figure 7-8 Trend of WSD reflection attack events

Figure 7-9 shows the global distribution of WSD reflection attack victims. We observed that up to 24 countries and regions were hit by this kind of attack. China was most targeted by WSD reflection attacks, home to 33% of victim IP addresses, followed by the USA (21%).

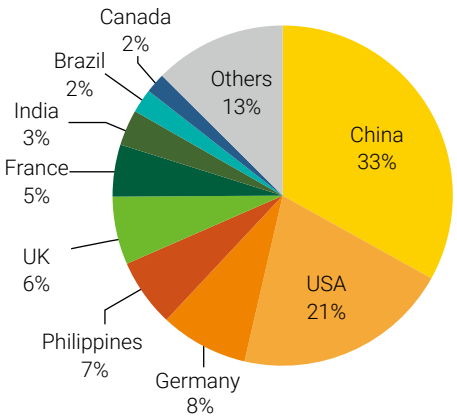


Figure 7-9 Global distribution of WSD reflection attack victims

7.2.3 Threats Against UPnP

UPnP is short for Universal Plug and Play. UPnP is an architecture that defines peer-to-peer connectivity of PCs and intelligent devices (or instruments). Built upon Internet standards and technologies (such as TCP/IP, HTTP, and XML), UPnP allows such devices to connect to and collaborate with each other automatically, thus making it possible for the network (especially home networks) to be accessible to more people. Therefore, many routers have this service that is publicly available. Within the UPnP protocol stack, Simple Service Discovery Protocol (SSDP) is used to discover devices in the local area network (LAN) and Simple Object Access Protocol (SOAP) is used for device control. For more basic knowledge of UPnP and vulnerability introduction, refer to NSFOCUS's *2018 Annual IoT Security Report*[1] .

As for devices with the UPnP SSDP service publicly available, China, South Korea, Venezuela, the USA, and Japan had the most such devices exposed. Meanwhile, we found that devices exposed in Russia registered a decrease of 84% as compared to 2018. It is estimated that related Russian authorities had pushed forward UPnP governance.

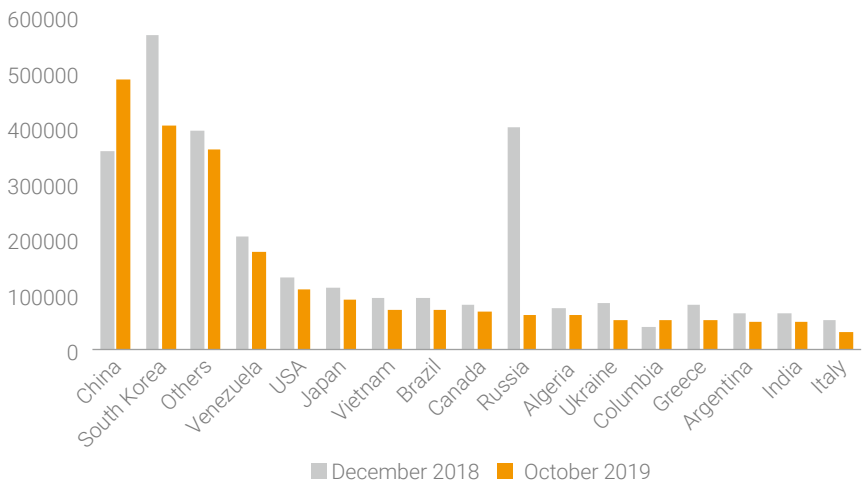


Figure 7-10 Global distribution of devices with the SSDP service publicly available

1 *2018 Annual IoT Security Report*, http://www.nsfocus.com.cn/content/details_62_2916.html

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

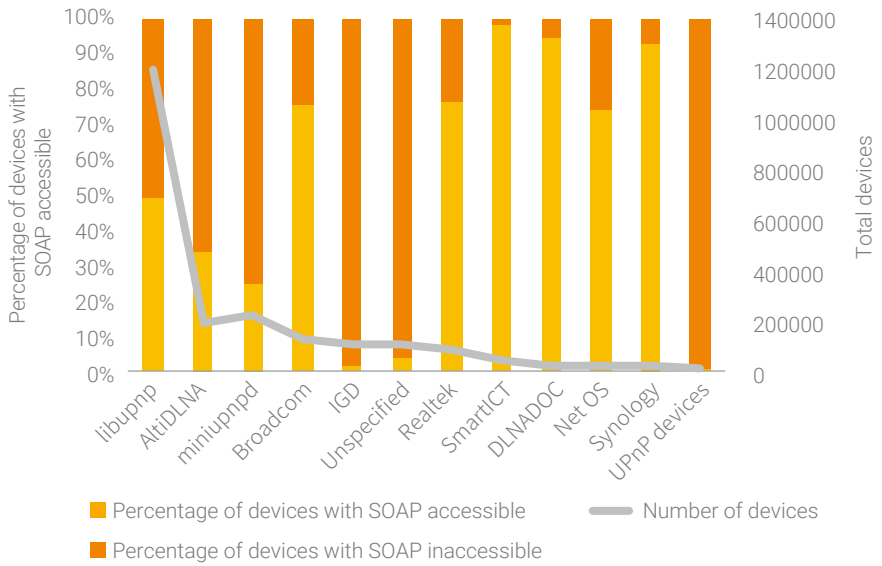


Figure 7-11 SOAP accessibility distribution of UPnP devices by SDK

Of 390,000 devices with port mapping publicly accessible, a total of 63,000 devices were found to be affected by more than one type of malicious behavior and some suffered several kinds of intrusions. Up to 45,000 devices experienced intranet intrusions and approximately 30,000 were detected to be broken into by a malicious proxy. Figure 7-12 shows the global distribution of devices with or without port mapping publicly accessible and the global distribution of such devices infected or uninfected with malicious behavior. China was home to the most devices with port mapping exposed and most devices infected with malicious behaviors.

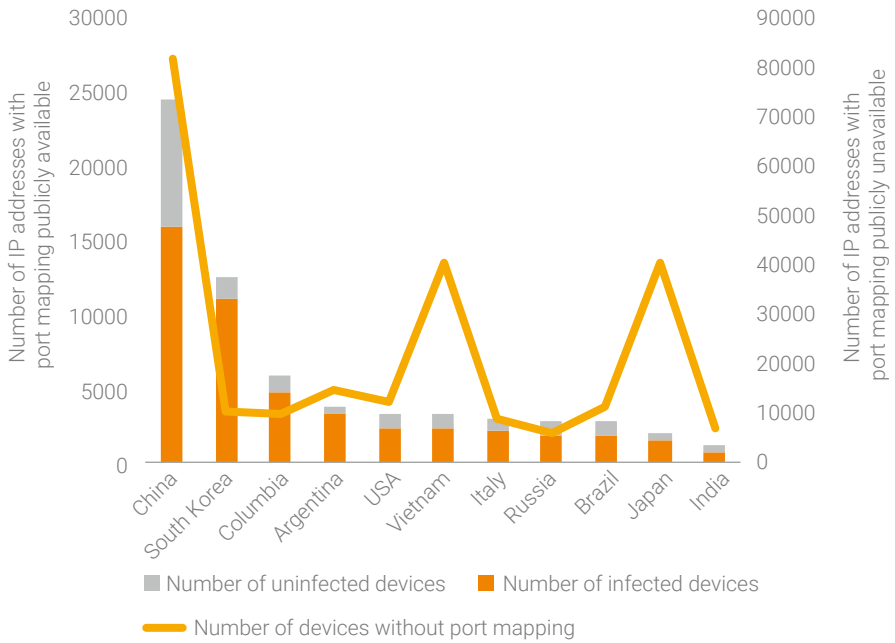


Figure 7-12 Global distribution of infected/uninfected devices with port mapping exposed

We captured four kinds of UPnP exploits[1] , as listed in Table 7.4. Apparently, all the exploits targeted remote command execution vulnerabilities. Besides, we found that when this vulnerability occurred at a specific port, attackers usually directly attacked this port by skipping the UPnP discovery phase.

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

Exploit Database No.	Vulnerability Disclosure Year	CVE ID	Vulnerability Description
No.	2017	CVE-2017-17215	Huawei Router HG532 - Arbitrary Command Execution
37169	2014	CVE-2014-8361	Realtek SDK - Miniigd UPnP SOAP Command Execution
37171	2015	CVE-2015-2051	D-Link Devices - HNAP SOAPAction-Header Command Execution
28333	2013	N/A	D-Link Devices - UPnP SOAP TelnetD Command Execution

Upon deduplication of source IP addresses indicated in UPnP logs, we found that about 29.6% of IP

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

addresses exploited UPnP vulnerabilities. We analyzed the global distribution of source IP addresses and discovered that China was home to the most attack sources. Our further analysis revealed that 90% of attacks in China were sourced from Taiwan and China Mainland had attack sources of the same order of magnitude as Russia and the USA.

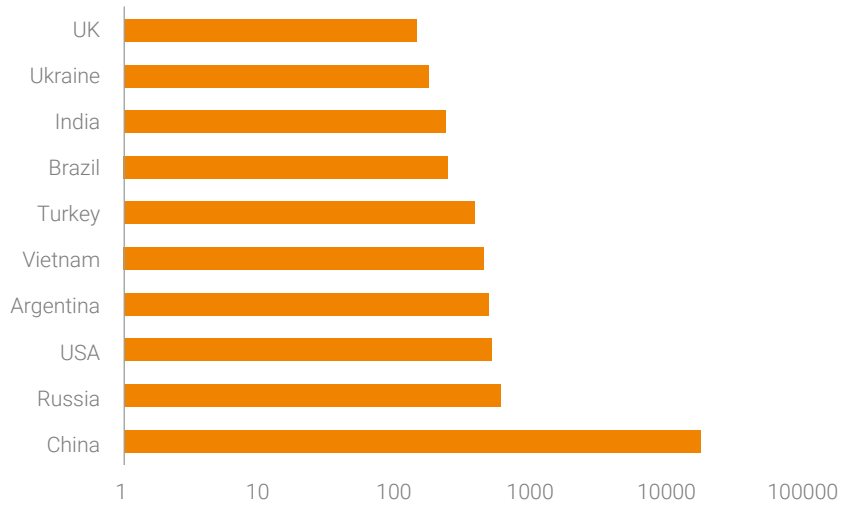


Figure 7-13 Global distribution of IP addresses of attack sources indicated in UPnP logs

8

Security Threats in the IPv6 Environment

Since the *Promoting Scale Deployment of Internet Protocol Version 6 (IPv6)* ("Plan") [1] was published in November 2017, IPv6 deployments in China are on the rise. By June 2019, the number of active IPv6 users had reached 130 million, and 1.207 billion telecom users had been assigned an IPv6 address. At the same time, IPv6 traffic in China in the past year steadily grew. The number of address resources ranked first in the world (47,282 IP address blocks (/32)) by May 2019. Telecom enterprises have made positive efforts to improve network infrastructure. All recursive domain name systems (DNS) of the three telecom magnates support IPv6 domain name resolution. Content delivery network (CDN) enterprises have conducted IPv6 deployments nationwide and have got the capability of accelerating distribution of IPv6 addresses. The transformation of backbone networks, LTE networks, and metropolitan area networks (MANs) has been almost completed[2] . With the rapid development of the IPv6 technology, more attention should be paid to security threats in the IPv6 environment. This section describes the threat situation from the perspectives of vulnerabilities and traffic.

8.1 IPv6 Vulnerability Trend

With the depletion of IPv4 addresses and since a World IPv6 Launch Day was carried out where countries permanently enabled IPv6 for their networks and applications in 2012, the deployment of IPv6-related systems, networks, and application services will be increasingly pervasive. So far, 25.33% networks have adopted IPv6 deployments[3] .

1 http://www.gov.cn/zhengce/2017-11/26/content_5242389.htm

2 http://www.caict.ac.cn/kxyj/qwfb/ztbg/201907/P020190712576587138174.pdf

3 https://stats.labs.apnic.net/ipv6/XA

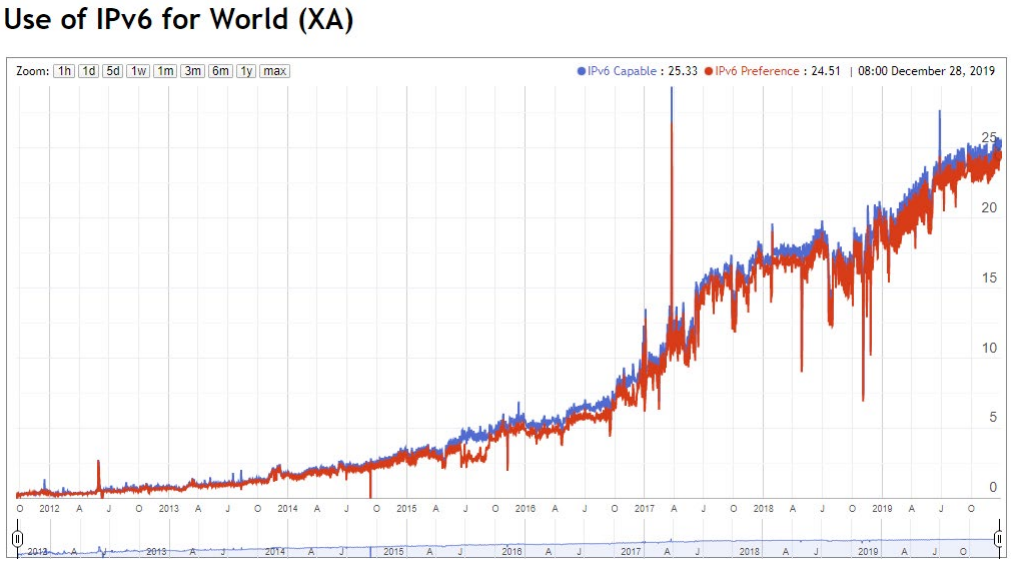


Figure 8-1 Global IPv6 adoption trend

With IPv6 networks and services going live, IPv6 system resources draw more and more attention from attackers. Amid this trend, IPv6-related vulnerabilities have gained momentum for rapid growth. Therefore, the Internet construction is facing severe security challenges. Compared with the IPv4 protocol, the IPv6 protocol is more secure, but the mechanism for transferring packets remains unchanged. As a result, IPv6 networks are still exposed to the same attacks as IPv4 networks. For example, HTTP attacks against the application layer and TCP attacks against the transport layer can also pose a serious threat to IPv6 networks. Since new fields and protocols are introduced, IPv6 packets are likely to contain vulnerabilities. For example, IPv6 extension headers, the Neighbor Discovery Protocol (NDP), and ICMPv6 protocol can be exploited by attackers for launching sniffing attacks and denial-of-service attacks. According to NVD statistics, a total of 369 IPv6 vulnerabilities have been detected since 2002.

Table 8-1 IPv6 vulnerability distribution

Protocol	Vulnerability Number	Vulnerability Type				Vulnerability Location			
		DoS	RCE	Information disclosure	Other	System	Application	Devices such as routers	Protocol
IPv6	369	244	3	20	87	187	113	23	1
ICMPv6	32	24	2	6	0	22	7	2	1
NDP	20	15	0	0	5	12	6	2	0
DHCPv6	33	27	1	3	2	14	18	1	0

Among all IPv6 vulnerabilities, denial-of-service vulnerabilities account for 60% (244), 185 of which are remote ones. DoS attacks can be devastating to network devices and services. Given the large proportion of DoS vulnerabilities, it will be an arduous task to defend against related attacks. It is noteworthy that the current IPv4 Internet is such a huge system that the economic and technical costs of migrating corresponding devices and application systems to the IPv6 Internet will be enormous. As a result, IPv4 and IPv6 networks will coexist for a long time. For smooth transition from IPv4 to IPv6, corresponding transitional techniques have been developed and put into practice, including dual stack, tunneling, and protocol translation. Security issues related to transitional techniques should also be considered. Currently, there are 16 vulnerabilities related to transitional techniques in the current vulnerability database. It is predictable that this number will increase in future.

8.2 Attack Type Distribution

In 2019, there were 295 types of alerts in the IPv6 network environment, reaching 2.37 million in total. Figure 8-2 shows the monthly trend of IPv6 alerts. As shown in the figure, IPv6 alerts were in the upward trend; in November, the number peaked at 880,000.

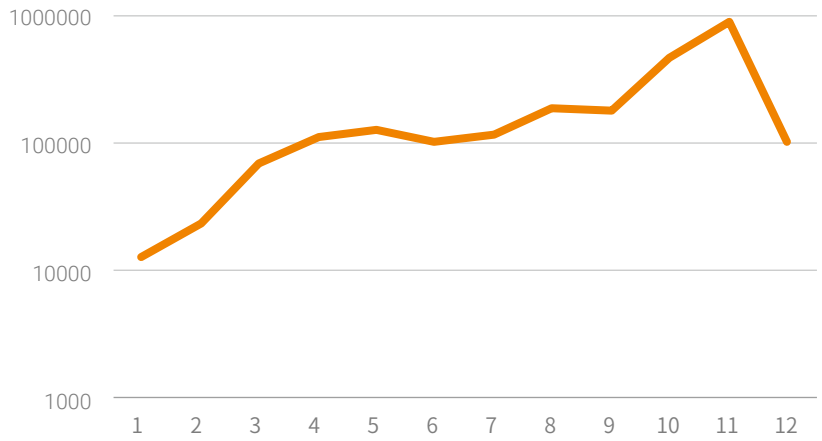


Figure 8-2 Monthly trend of IPv6 alerts

Malware

Backdoors and cryptojacking malware are the most frequently detected malware, followed by trojans, ransomware, and worms.

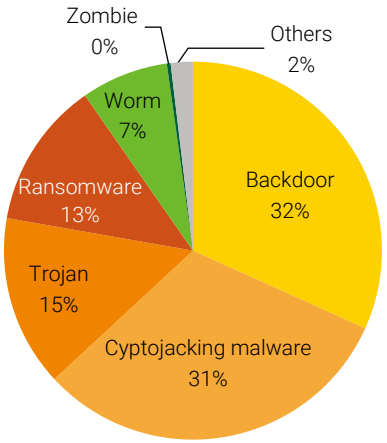


Figure 8-3 Distribution of IPv6 malware by type

In 2019, most alerts were generated on backdoors in the IPv6 environment, accounting for 32%. Figure 8-4 shows the daily trend of backdoor attacks. June and July saw the most back alerts, and several daily peaks were formed. Most alerts were generated in early July, peaking at 1633 in a day.

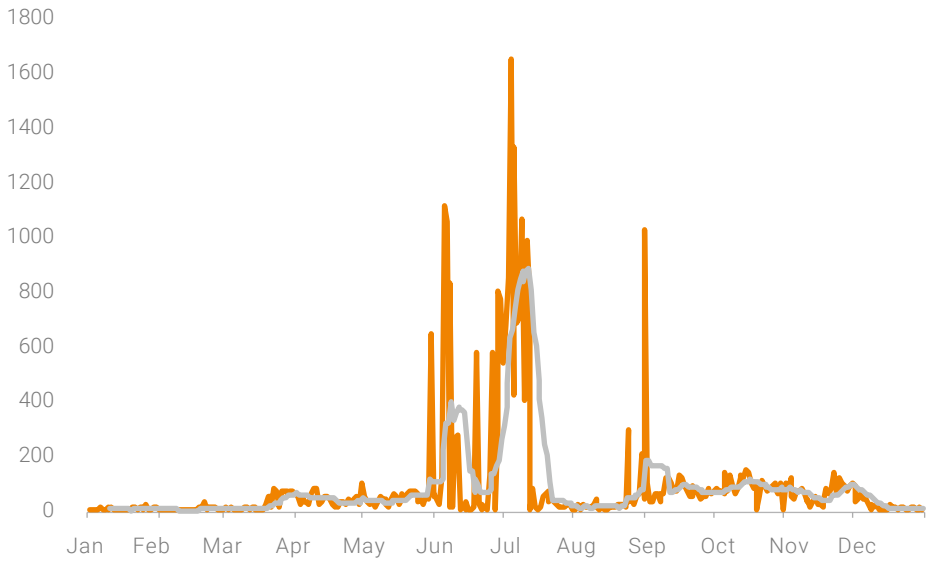


Figure 8-4 Trend of backdoor attacks

Table 8-2 lists top 5 types of backdoor attacks. It is worth noting that 27,500 alerts were generated on suspicious web shell backdoor access control attacks, contributing 87.8% of all trojan attacks.

Table 8-2 Top 5 types of backdoor attacks

Top 5 Alert Types
Suspicious web shell backdoor access control
Trojan backdoor Chopper web shell detection
PHP-based one-line trojan
WinterLove communication 2
CMS splitword.php backdoor

In the IPv6 environment, cryptojacking alerts accounted for 31%, second only to backdoors. As shown in Figure 8-5, cryptojackers in the IPv6 environment had a lower level of activity in early 2016. Then the number of alerts increased slowly but burst in late June. At the end of 2019, there were a large number of IPv6 cryptojacking alerts. Late June and early July saw the most cyptojacking activities. The peak period lasted for nearly a month.

Figure 8-5 Cyptojacking trend

Table 8-3 lists top 5 cryptojacking activities. Most alerts were generated on WannaMine connection communication and WannaCry attempted communication, followed by Monero (XMR) cryptominer network communication, malicious cyrptominer XmrigDNS request connection, and cyrptominer query DNS mining pool server domain name.

Table 8-3 Top 5 cryptojacking activities

Alert Name
WannaMine Connection Communication
WannaCry Attempted Communication
Monero (XMR) Cryptominer Network Communication
Malicious Cyrptominer XmrigDNS Request Connection
Cyrptominer Query DNS Mining Pool Server Domain Name

Web Attacks

In terms of attacked applications, web services were the major attack target, accounting for 44%, followed by DNS services (42%).

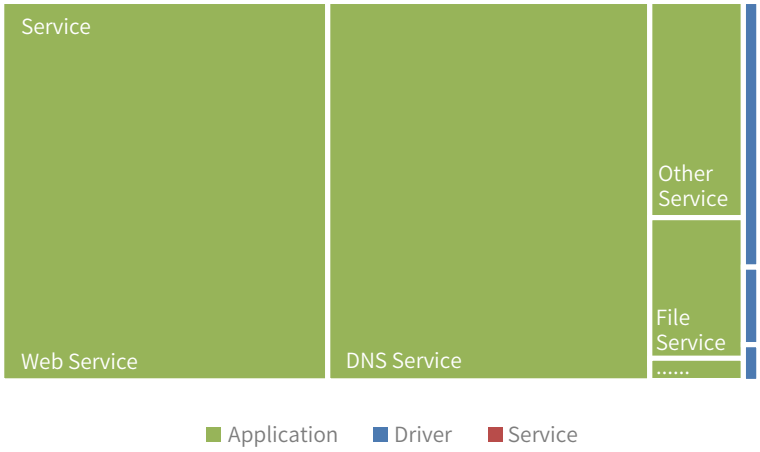


Figure 8-6 Proportions of attacked applications by type

Table 8-4 lists top 5 attacked web frameworks. Tomcat and ThinkPHP received the most attacks, followed by Internet Information Services (IIS), Struts, and Nginx.

Table 8-4 Top 5 attacked web frameworks

Attacked Web Framework
Tomcat
ThinkPHP
IIS
Struts
Nginx

Remote cross-site scripting attacks were still the most common web attacks, an increase of 10 times from 2018.

Table 8-5 Top 10 web attacks

Number of Alerts	Alert Name
85621	Web Service Remote Cross-site Scripting Attack
50319	Web Service Remote SQL Injection Attack Suspicious Behavior
23103	JavaScript Obfuscation Code in HTML
16984	PHP Code Execution Vulnerability
13622	HTTP/2HEADERS and CONTINUATION Frame Connection
10953	HTTPURLTab Character Splitting Evasion Attempt
6292	Java Code Execution Vulnerability
5812	ApacheTomcat Remote Code Execution Vulnerability (CVE-2017-12615)
5346	FCKeditor FileUpload() Arbitrary File Upload Vulnerability
3798	HTTP Command Injection Attempt
3230	ThinkPHP 5.x Remote Command Execution Vulnerability

8.3 Geographical Distribution of Attack Sources

According to the analysis of geographic distribution of IPv6 attack sources, China had the largest proportion of attack sources (86.76%), followed by the USA (3.97%) and Romania (0.77%).

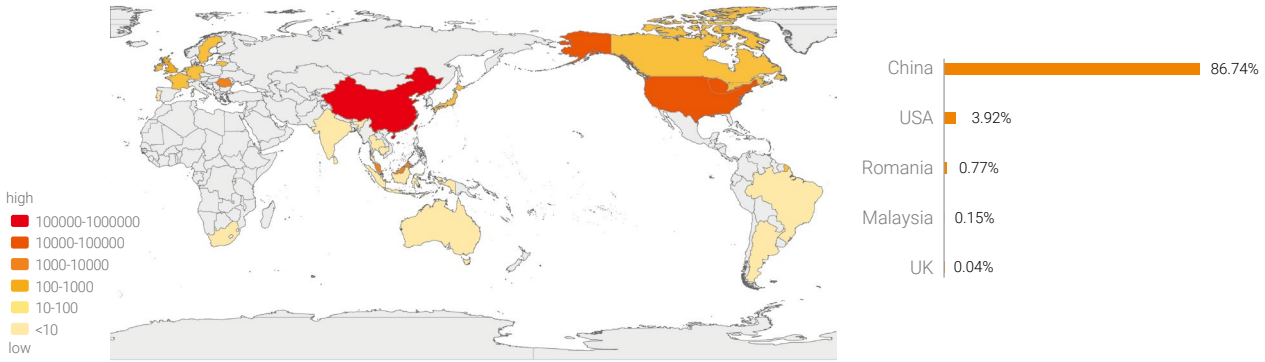


Figure 8-7 Global distribution of attack sources

As shown in Figure 8-7, China was home to the largest number of attack sources.

9

Conclusion

In 2019, as the data breach situation was more severe than previous years, data security protection battles grew more and more intense. Trends in legislation and law enforcement suggest that governments at home and abroad are taking proactive measures. For enterprises, compliance has become a top security concern.

DDoS attackers were powered by maturing techniques. Multi-vector volumetric attacks posed a greater challenge to defense operations. Amid DDoS attack incidents, behaviors of active gangs deserve special attention. Besides, the number of IoT devices involved in DDoS attacks increases year by year as a result of hackers finding their way into IoT devices via Telnet, repeatedly and successfully, further dampening the cybersecurity landscape.

The IPv6-based Next Generation Internet (NGI) will become the cornerstone to support the rapid development of cutting-edge technologies and industries. Amid this trend, IPv6-related vulnerabilities are on the rise. Besides, application-layer attacks using IPv6 addresses have become the simplest and most efficient attack method. For managers in charge of IPv6, the first priority is to follow up with the evolution of traditional security threats in IPv6 environments.

As mobile payment and mobile office are increasingly popular, mobile devices have become common constituents of the APT attack surface. APT groups still take phishing as the major means at the intrusion stage and have never slackened their pace of updating their toolkits and improving their attack methods. Worse still, they collude with other botnet owners. Predictably, botnets will open the door for APT attacks.

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com