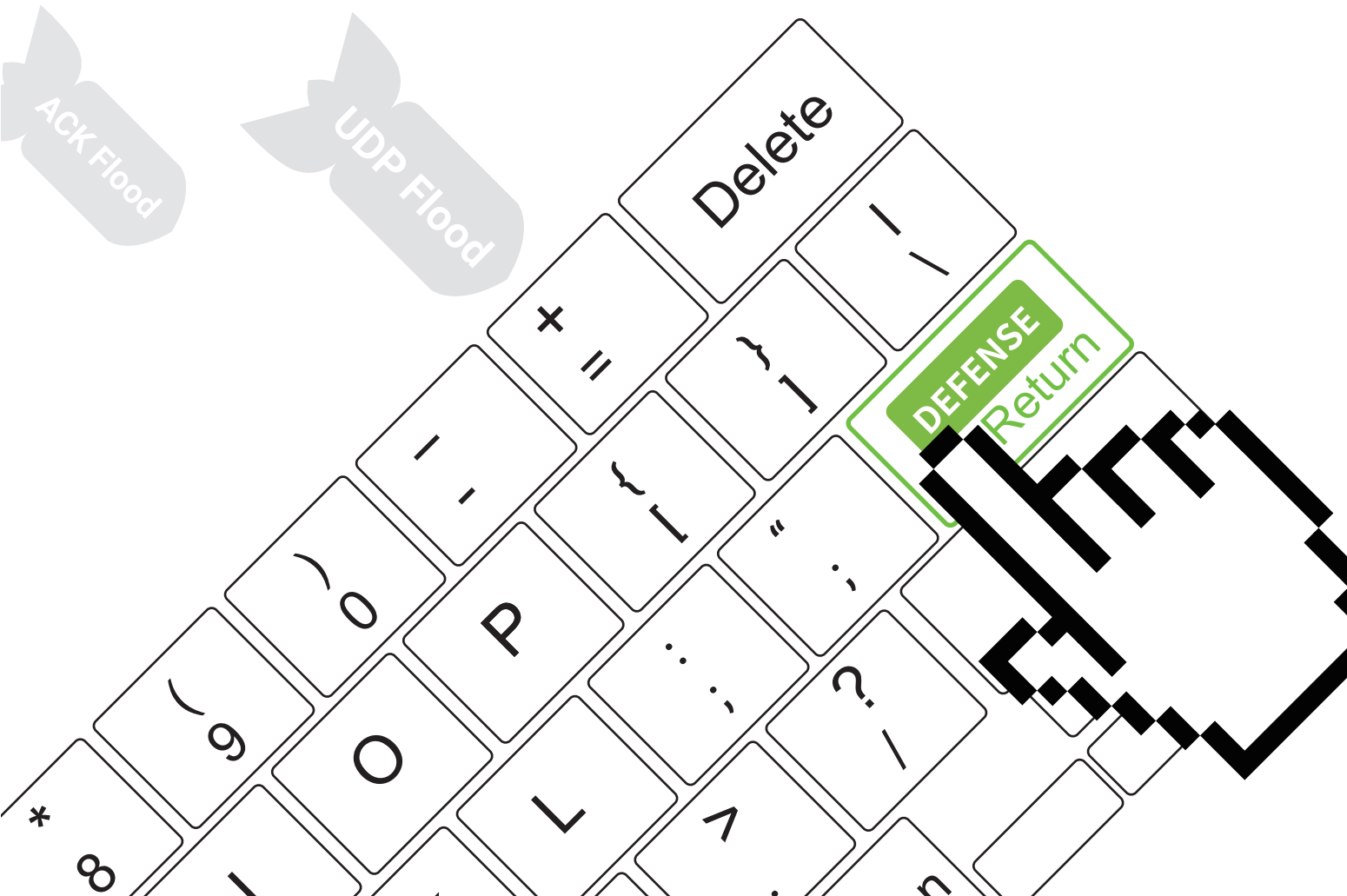
2019

DDoS Attack Landscape

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

In 2019, the average peak size of DDoS attacks rose steadily from 2018 to 42.9 Gbps, indicating that techniques employed by large and medium scale attacks are advancing year by year. After a sharp rise in 2018, super-sized DDoS attacks (> 300 Gbps) were relatively stabilizing in 2019, increasing slightly by around 200.

On the other hand, the total traffic of DDoS attacks in 2019 declined 26.4% compared with 2018, a signal that more mature attack techniques do not make attackers more inclined to launch DDoS attacks. The booming of the Bitcoin market and the functional migration of botnets may be the main reasons behind this. Botnets go far beyond DDoS attacks and remote controls. Attackers may choose to combine botnets with ransomware or cyptomining trojans for attacks or use botnets for distributed cracking. With full-featured attack tools readily available on black and grey markets, attackers are capable of following the market trend closely to maximize their illegal gains.

At the same time, Internet of Things (IoT) devices are making more presence in DDoS attacks. Throughout the year of 2019, approximately 170,000 IoT devices were found in DDoS attacks. Of all DDoS gangs we have detected, one gang contains 28,000 IoT devices, among others, available for various attacks, accounting for 31% of the total number. IoT devices are massive in quantity. Besides, they stay connected in most of the time and often contain vulnerabilities that fail to be addressed in time. For these reasons, they become the hotbed of exploits, making it an urgent need to enhance people's security awareness and make more efforts in prevention and governance of related threats.

Chapter 2 presents an overview of DDoS attacks in 2019. In chapter 3, we, from perspectives of attack resources, gang behavior, IoT, and botnets, anatomize the changes and evolution of DDoS attacks in 2019 in terms of attack counts, traffic, types, time, and locations, in hopes of helping organizations make informed decisions on how to continuously improve their network defense systems and techniques.

2

Overview of DDoS Attacks in 2019

2.1 2019 vs. 2018

- The total attack count increased 30.2%, but the total traffic declined 26.4%.
- The number of small-scale attacks (1–5 Gbps) increased greatly, and that of large-scale attacks (> 300 Gbps) grew slightly.
- The average attack peak size rose a little to 42.9 Gbps and the technical maturity of large- and medium-scale attacks has grown year by year.
- UDP floods, SYN floods, and ACK floods still dominated DDoS attacks, and, in super-sized attacks, those combining multiple vectors stole the limelight.
- IoT devices were more frequently seen in DDoS attacks.
- The exploit payload of IoT botnet families in 2019 shared similarities with that in 2018, mainly targeting smart IoT devices. Meanwhile, attack methods were diversified and a trend of assigning different jobs to different roles on the kill chain took shape.

2.2 Key Findings

- Maturity: The technical maturity of attackers keeps growing, opening more possibilities than DDoS attacks for attackers to garner profits.
- 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.
- 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.
- 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.

- 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.
- 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.

3

Analysis of DDoS Attacks in 2019

3.1 DDoS Attack Counts and Peak Sizes

3.1.1 Distribution of Peak Sizes

From the monthly data in the last three years, the number of large-scale attacks (> 100 Gbps) soared in 2018 and then fluctuated at a high level over a two-year period. In 2017, the number of such attacks reached 11,800, only 48% of the number in 2018 (24,500). 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.

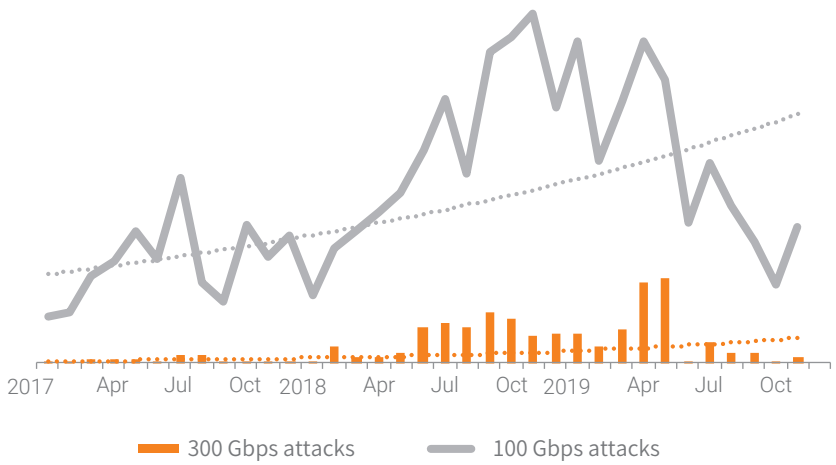


Figure 3-1 Monthly number of high-volume DDoS attacks in the last three years

Of all DDoS attacks, 22.2% peaked at 1–5 Gbps, making up the largest proportion. Compared with 2018, 2019 saw more DDoS attacks with small peak sizes. Those peaking below 10 Gbps increased slightly to account for 49.9% and attacks peaking at 1–5 Gbps increased multiple times.

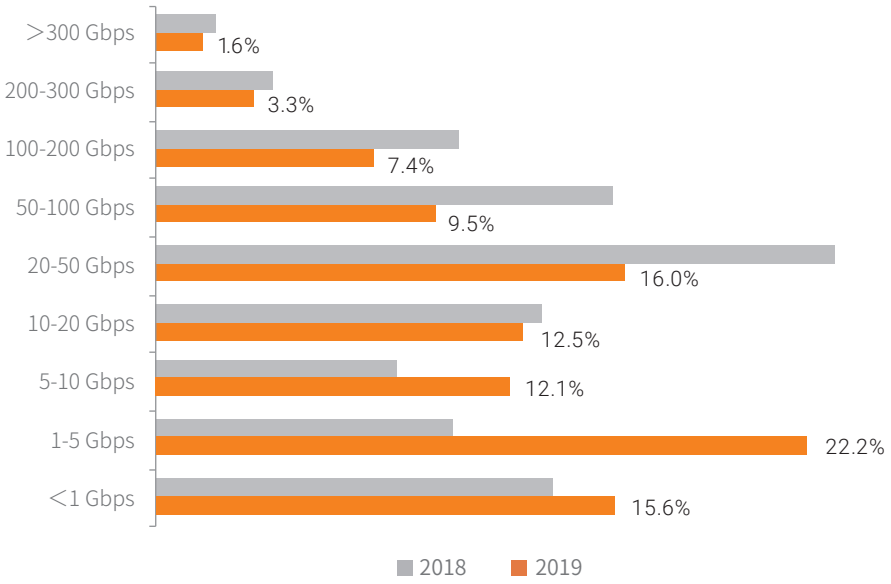


Figure 3-2 Distribution of attack peak sizes

On a quarterly basis, small-scale DDoS attacks peaking below 20 Gbps have continued to grow. In 2019 Q4, small-scale attacks made up 66% of all DDoS attacks detected in this quarter, and in Q2 of this year, small-scale attacks peaking below 5 Gbps accounted for 41.5%. Super-sized attacks (> 300 Gbps) declined in proportion, but rose slightly in number. By November 2019, altogether 2894 such attacks had been spotted, a bit more than 2018 (2673). By contrast, 2017 saw only 350 such attacks. Compared with this figure, super-sized attacks in the last two years have increased more than 7 times.

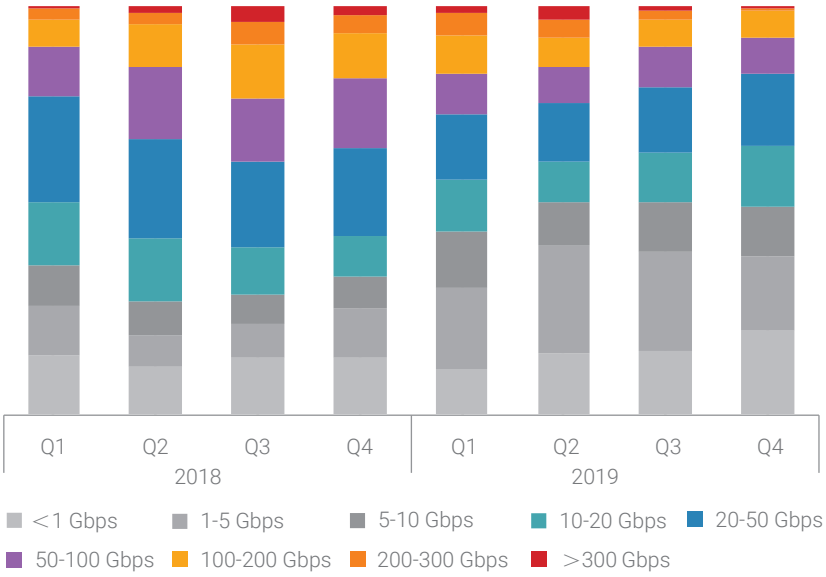


Figure 3-3 Quarterly proportions of DDoS attacks of various scales in 2018 and 2019

3.1.2 Attack Counts and 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.

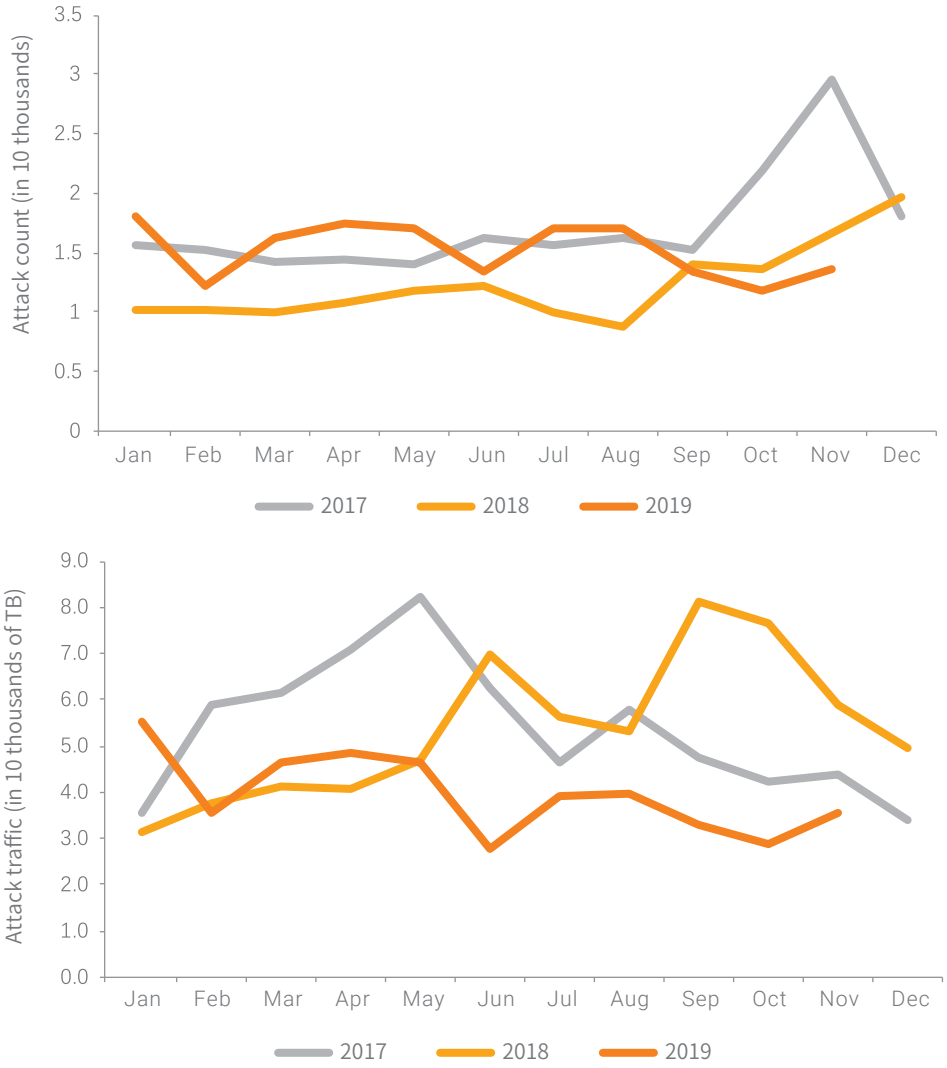


Figure 3-4 Monthly attack counts and traffic over a three-year period

In terms of the monthly attack count, DDoS attacks stabilized in 2019. In terms of the attack traffic, DDoS attacks began to take a downslide turn in the latter half of the year. We believe that the overall trend of DDoS attacks was linked with the rise of cryptocurrency price. In the 2017 DDoS and

Web Application Attack Landscape[1], we pointed out that, with the appreciation of cryptocurrency, hackers on the black market began to divert prime botnet resources to cost-efficient cryptomining activities from costly DDoS attacks. In 2019, with a pickup in cryptocurrency prices, cryptomining became more lucrative. In this context, attackers were less inclined to launch DDoS attacks to garner profits, which was especially the case in the latter half of the year.

Comparing the monthly Bitcoin price with the monthly DDoS attack traffic, we get the Pearson correlation coefficient of –0.53, indicating a negative correlation between the two, which attests to the truth of our viewpoint given before.

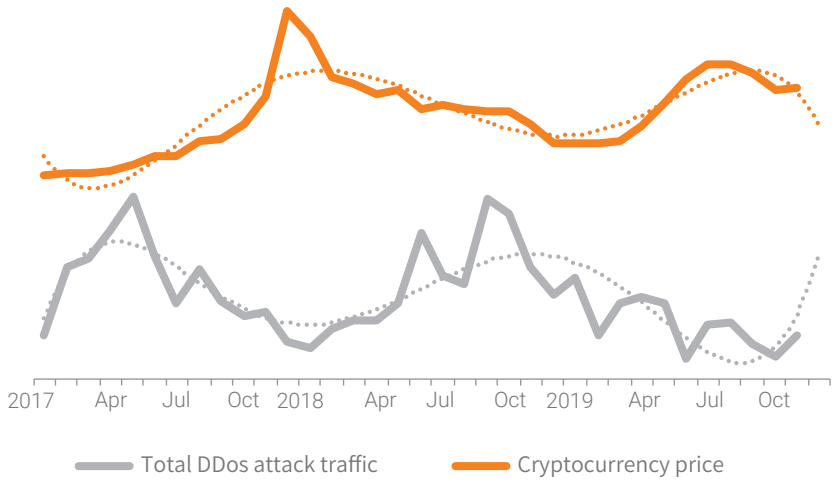


Figure 3-5 DDoS attack traffic correlation with Bitcoin prices

3.1.3 Maximum and Average Peak Sizes of Individual Attacks

At the beginning of 2019, new DDoS attack tools came into view. For example, in early February, a fast evolving botnet Cayosin[2] made up of devices infected with QBot, Mirai, and other malware

1 https://nti.nsfocus.com/pdf/2017_DDoS_and_Web_Application_Attack_Landscape_en.pdf

2 https://cyware.com/news/newly-discovered-cayosin-botnet-leverages-social-media-platforms-for-propagation-3f8adcd1

families grabbed people's attention because of widely spreading through such media as YouTube. In mid-March, a variant of Mirai[3] surfaced, boasting a larger database of exploits besides broadening its scope of targets.

According to data collected by November 2019, the average peak size of DDoS attacks in 2019 was 42.9 Gbps, on a par with that in 2018 over the same period (41.1 Gbps). In the first half of 2019, the average peak size per month was virtually larger than that over the same period of 2018. However, starting from July, 2019 lagged behind of 2018 in the average peak size per month.

In terms of the maximum attack peak size, from January to May, the curve of 2019 was above that of 2018, but starting from June, the two curves changed positions. In 2018, the maximum peak size of 1.41 Tbps was captured in June. In 2019, the maximum peak size stood at 885 Gbps, spotted in May.

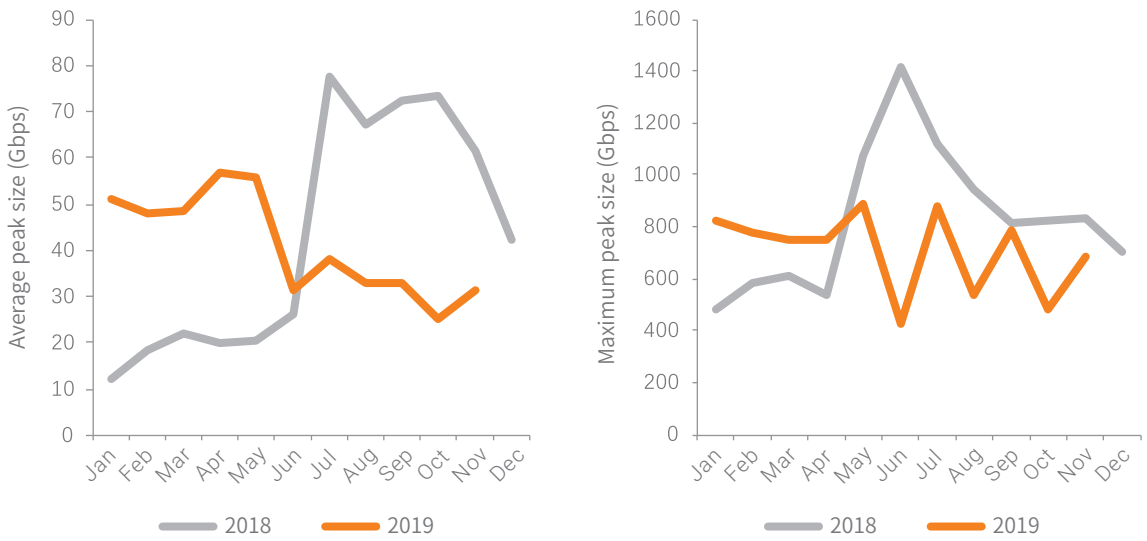


Figure 3-6 Average monthly peak sizes and maximum monthly peak sizes in 2018 and 2019

3 https://www.chainnews.com/zh-hant/articles/153084039107.htm

3.2 DDoS Attack Type Analysis

3.2.1 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.

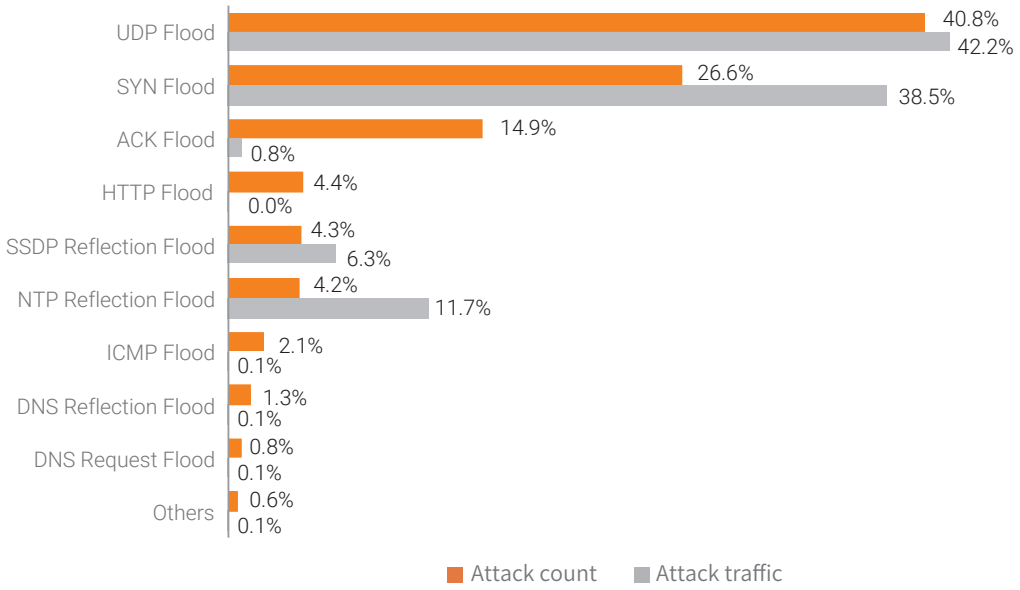


Figure 3-7 Proportions of different attack types by count and traffic

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

UDP floods, SYN floods, and ACK floods still dominated DDoS attacks. By contrast, the proportion of HTTP flood attacks decreased to 0.1% from 8.3% in 2018.

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. Another thing to note about multi-vector attacks is that they stood out from super-sized attacks in 2019, second only to SYN attacks. For details, see section 3.2.2 Distribution of Attack Types by Consumed Bandwidth.

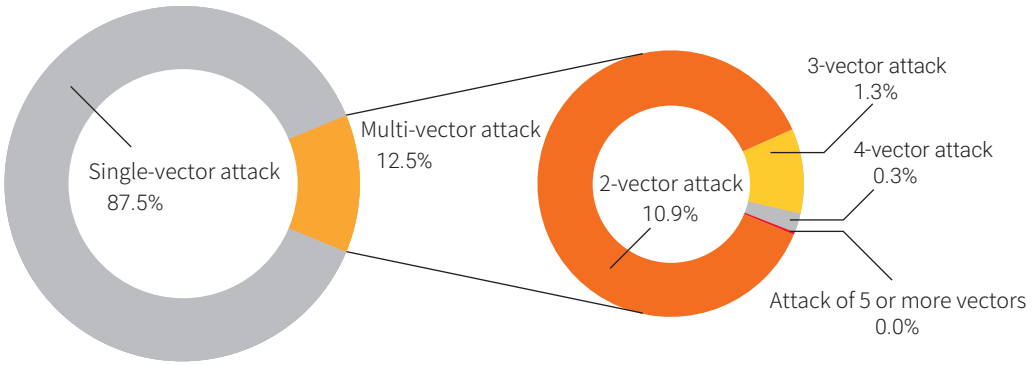


Figure 3-8 Distribution of multi-vector attacks

Source: NTI and Cloud DPS

Typical case:

In August 2019, a customer of Cloud DPS in the gaming industry experienced persistent high-volume DDoS attacks in one month, including more than 20 attacks that peaked above 200 Gbps. The maximum peak size hit 388.5 Gbps. After Cloud DPS filtered out attack traffic, the normal traffic was only 110.6 Mbps, taking up less than 0.1% of the total traffic.

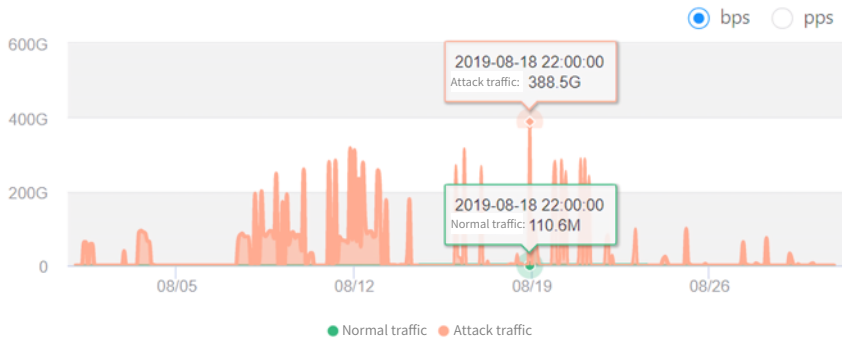


Figure 3-9 Traffic profile of a gaming-industry customer under attack

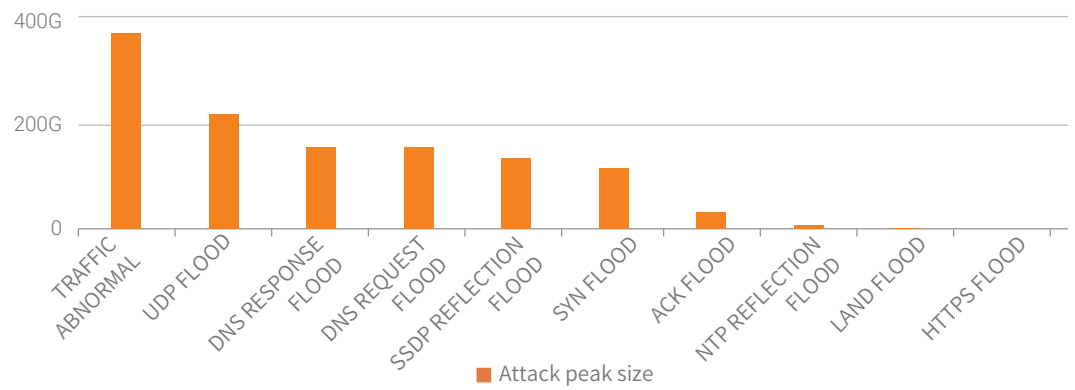


Figure 3-10 Peak sizes of multi-vector attacks

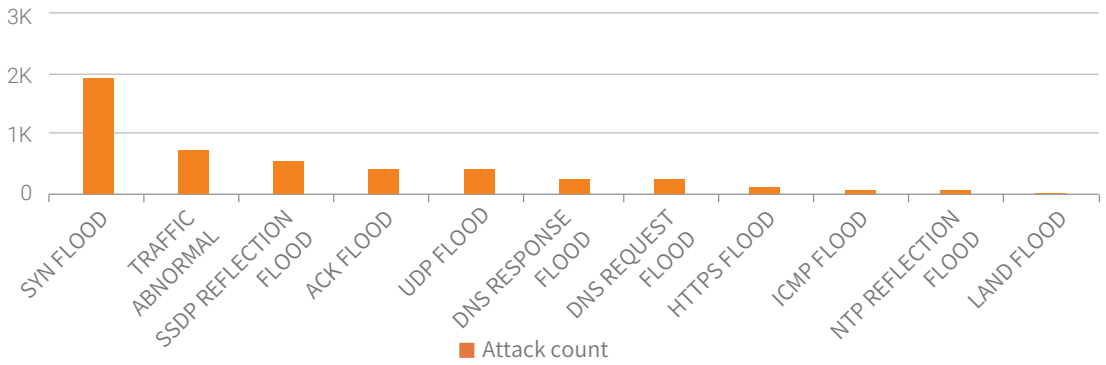


Figure 3-11 Counts of multi-vector attacks

Source: NTI and Cloud DPS

The attacks were focused on the customer's two network segments, with the following characteristics:

One network segment was mainly under attack of various UDP floods, including common UDP floods and distributed reflective denial-of-service (DRDoS) attacks that have been prevalent in recent years such as NTP reflection, SSDP reflection, and SNMP reflection attacks. DRDoS attacks are often conducted via large quantities of source IP addresses worldwide to generate

over 200 Gbps traffic in scores of minutes to about one hour. In a reflection attack, source ports, with obvious signatures, can be blocked with simple protection rules. What is put to the test is not detection algorithms, but the coverage of the cleaning equipment room, the stability of cleaning lines, and the performance of cleaning devices.

The other network segment was subject to empty connection attacks that peaked at only around 100 Gbps, but were capable of bypassing conventional TCP protection algorithms. By capturing and analyzing packets, security experts discovered the pattern of these attacks: A zombie sends a TCP connection request to the server, which responds as expected. After the TCP three-way handshake is complete, the zombie immediately sends FIN and RST packets to re-initiate the connection, thereby consuming server resources. This type of attacks puts to the test the defense operations service provider's response speed, promptness of dynamic policy adjustment, and security experience.

3.2.2 Distribution of Attack Types by Consumed Bandwidth

In 2019, SYN flood attacks overtook UDP flood attacks to contribute the largest proportion of volumetric attacks.

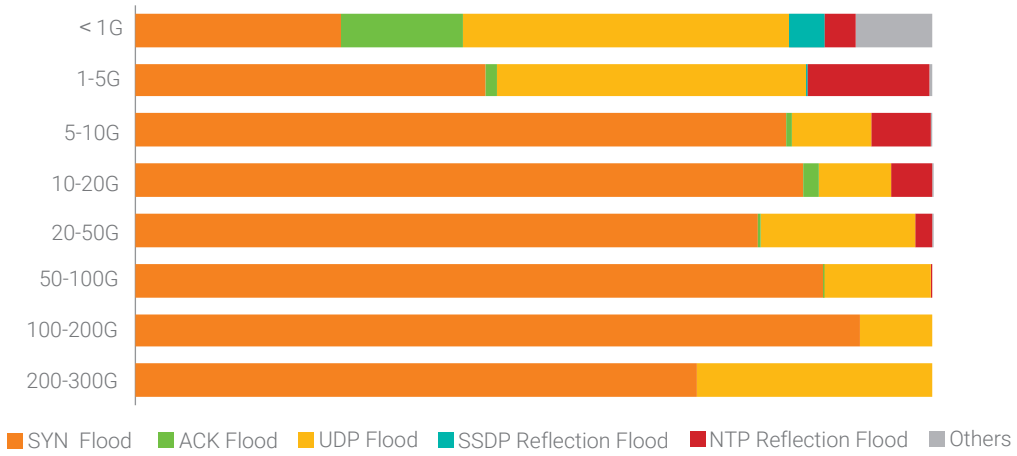


Figure 3-12 Distribution of DDoS attack types by consumed bandwidth

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.

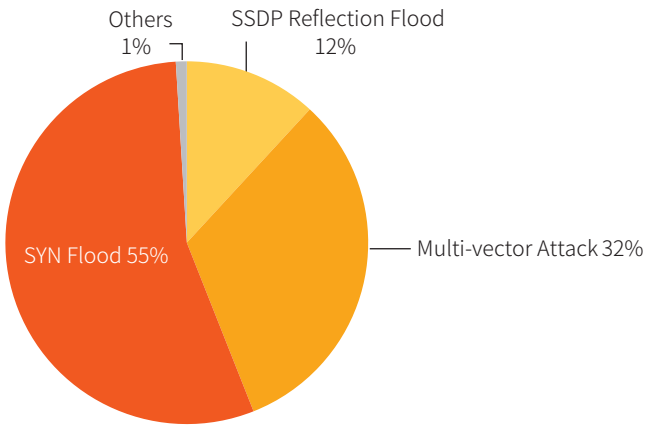


Figure 3-13 Distribution of super-sized attack types (> 300 Gbps)

3.2.3 Reflection Attacks

In 2019, the number of reflection attacks took up 10% of the total DDoS attacks, but related traffic accounted for 18% of the total DDoS traffic. Due to their amplification effect, reflection attacks are still a hazard that cannot be ignored. Besides, continuous attention should also be paid to emerging reflection attack types. According to the in-depth analysis of WS-Discovery reflection attacks by NSFOCUS Security Labs in the latter half of 2019, there were about 910,000 IP addresses around the world that had the WSD service publicly accessible, thus exposing themselves to the risk of DDoS attacks (the reflection factor could be as high as 500). Of all these devices, 80%, or 730,000, were video surveillance devices.

In terms of the attack count, NTP reflection and SSDP reflection attacks dominated reflection attacks, together accounting for 84%. In terms of the attack traffic, NTP reflection attacks stood out, contributing 65% of all reflection attack traffic.

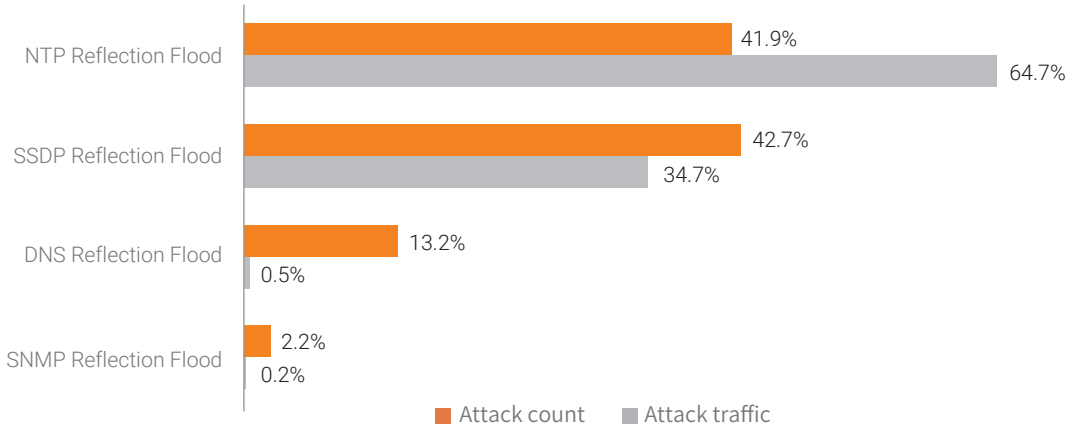


Figure 3-14 Proportions of various reflection attacks by count and traffic

3.3 DDoS Attack Time Profiling

3.3.1 Attack Distribution by Duration

In 2019, the average duration of DDoS attacks was registered at 52 minutes, an 18% increase from 2018. We noticed that the longest DDoS attack in 2019 lasted around 20 days, far longer than attacks detected in previous years.

In 2019, a DDoS attacks lasting less than 30 minutes accounted for 75%, approximate to the figure registered in 2018. The high proportion of short attacks signals that attackers are attaching more and more importance to the attack cost and efficiency and are more inclined to overwhelm the target service with floods of traffic in a short time, getting users offline and causing high latency and jitters. In addition, Botnet-as-a-Service (BaaS) and DDoS-as-a-Service (DDoS) have gained momentum for rapid development, which were also to blame for the prevalence of short attacks. Thanks to their availability, platform users are able to launch massive attacks in a very short time as long as they are willing to pay a certain amount of money for a whole lot of mercenary attack

resources[4]. In the long run, repeated burst attacks, which are under effective cost control, will greatly aggravate the quality of target services.

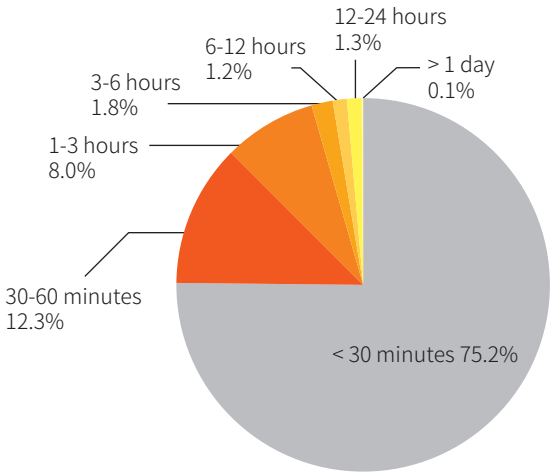


Figure 3-15 Proportions of attacks by duration

3.3.2 Temporal Distribution of Attack Activities Intraday

In one day from 0:00 to 24:00, busy hours (10:00–22:00) of services were the peak period of DDoS attacks, when 70% of attacks were spotted. The coincidence of busy hours of online service access with the peak period of DDoS attacks indicates that attackers intended to maximize their attack effect and impact.

4 http://blog.nsfocus.net/gafgy-botnet-baas/

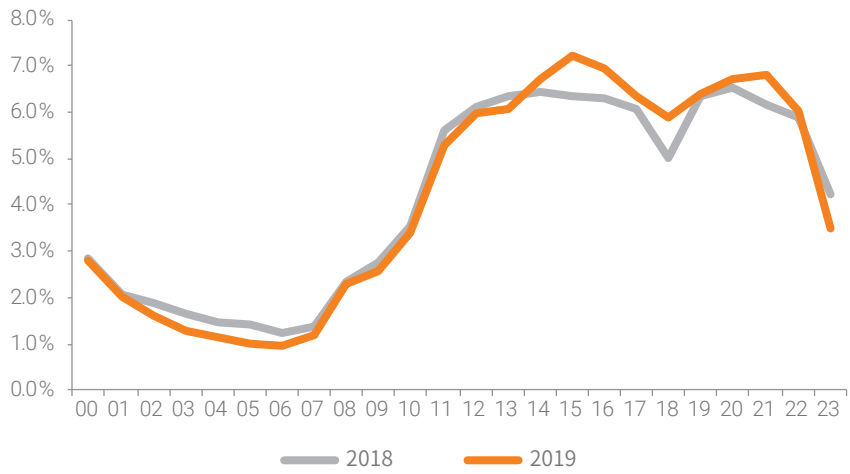


Figure 3-16 Temporal distribution of intraday DDoS attacks in 2018 and 2019

3.3.3 Temporal Distribution of Attack Activities Intraweek

In a week from Monday to Sunday, DDoS activities were evenly distributed in the seven days. An important reason behind this is that current network service providers usually serve customers 24/7. The odds of being attacked are the same for all the seven days.

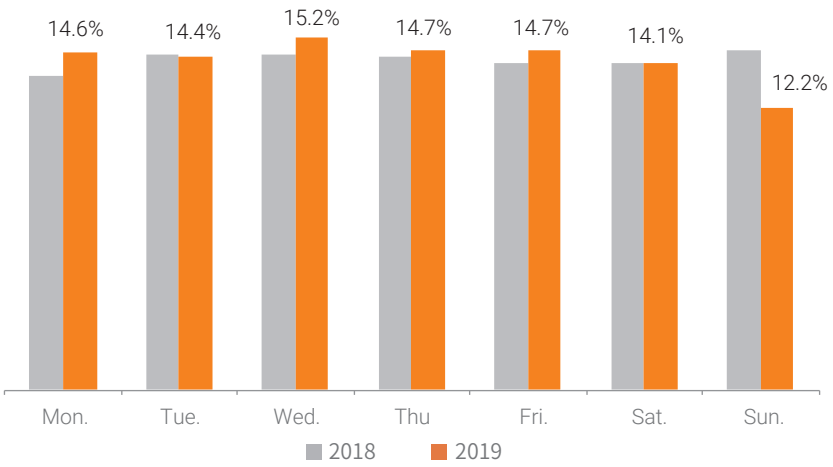


Figure 3-17 Temporal distribution of intra week DDoS attacks in 2018 and 2019

3.4 Geographical Distribution of DDoS Attacks

3.4.1 Controlled DDoS Attack Sources

According to statistics, China was still home to the largest number of controlled DDoS attack sources (36.19%) in 2019, followed by the USA and UK. Although China's ranking remained unchanged in terms of the number, the proportion decreased compared with 2018. This indicates that China's DDoS governance and defenses have yielded fruits.

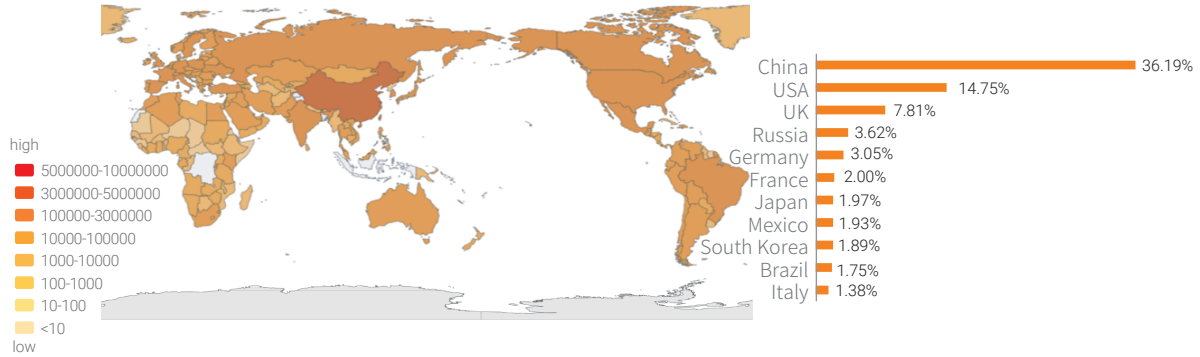


Figure 3-18 Distribution and proportions of attack source IP addresses in top countries

Source: NTI and Cloud DPS

3.4.2 DDoS Attack Targets

In 2019, the USA was the most severely attacked country, seeing 47.68% of DDoS attacks, followed by China (12.13%).

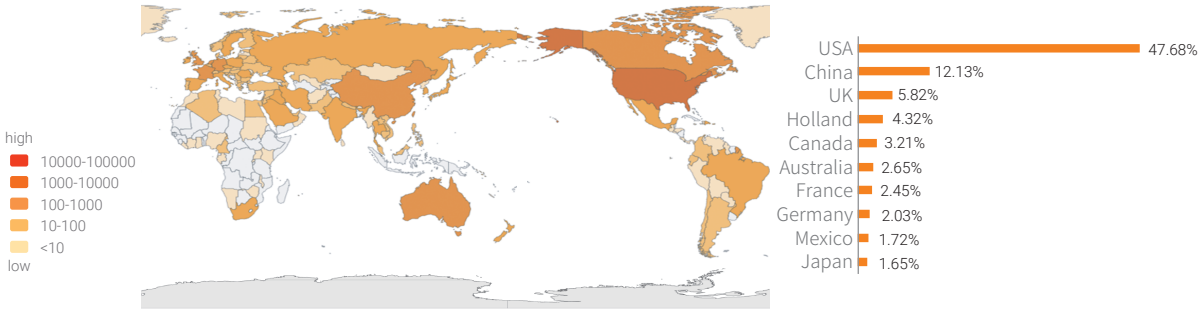


Figure 3-19 Distribution and proportions of attacked IP addresses in top countries

Source: NTI and Cloud DPS

3.4.3 DDoS Control Servers

Globally, the USA, China, and Holland were top 3 countries with the largest number of IP addresses of DDoS control servers, making up 53.13% of the world's total.

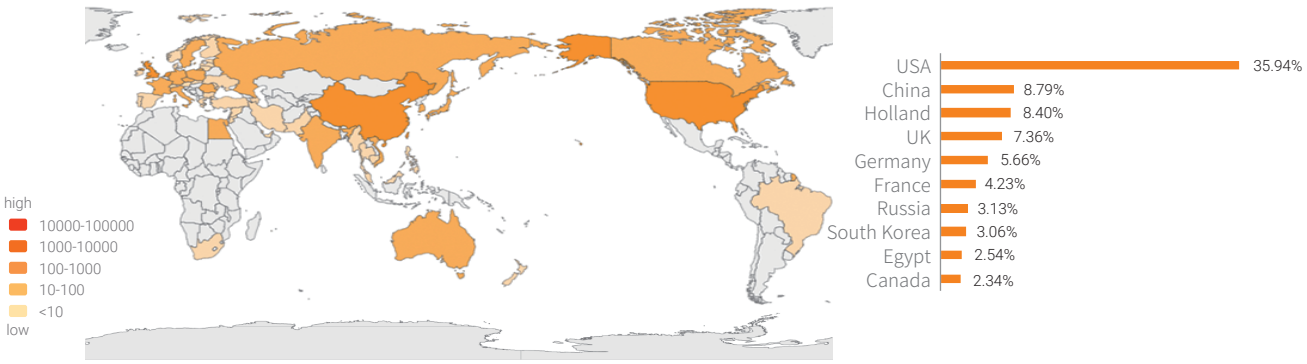


Figure 3-20 Distribution and proportions of control servers in top countries

Source: NTI

3.5 Behavioral Analysis of Attack Sources

3.5.1 Activity of Attack Sources

Ongoing monitoring of attack sources reveals that 90% of them were active for no longer than 10 days. There were two reasons behind this. For one thing, in order to keep attack sources fresh and prevent them from being blacklisted by defenders, attackers tended to use the hit-and-run strategy. For the other, there were a lot of vulnerable IP addresses widely distributed on the Internet, which could be easily obtained at a very low cost. Moreover, the proportion of IoT devices in attack sources that were active for more than 10 days rose sharply to 11.5%.

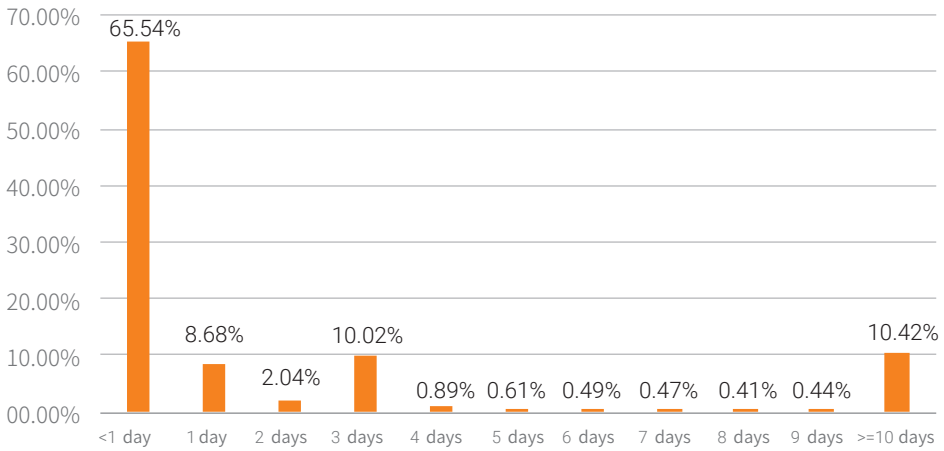


Figure 3-21 Proportions of short-lived attack sources

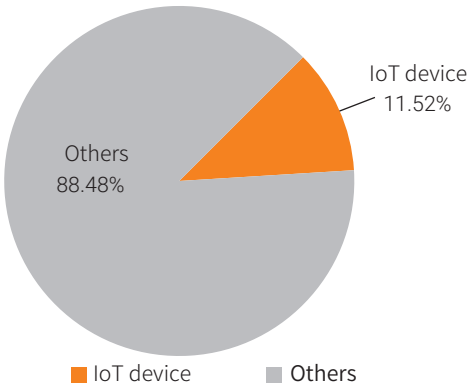


Figure 3-22 Proportion of IoT devices in long-lived attack sources

Source: NTI and Cloud DPS

3.5.2 Geographical Distribution of Active Attack Sources

Based on the activity duration, attack sources active for over 10 days are regarded to be highly active. These IP addresses often contain obvious and easily exploitable security hazards that can pose very severe threats.

Globally, highly active attack sources were mostly distributed in China, the UK, and the US. In China, they were mostly found in coastal provinces and economically developed regions, such as Zhejiang, Jiangsu, Guangdong, and Shandong. With a larger base of infrastructure, networks in these regions are more vulnerable than in other regions, provided that the same level of protections is deployed, because of hosting a much larger number of potentially vulnerable devices.

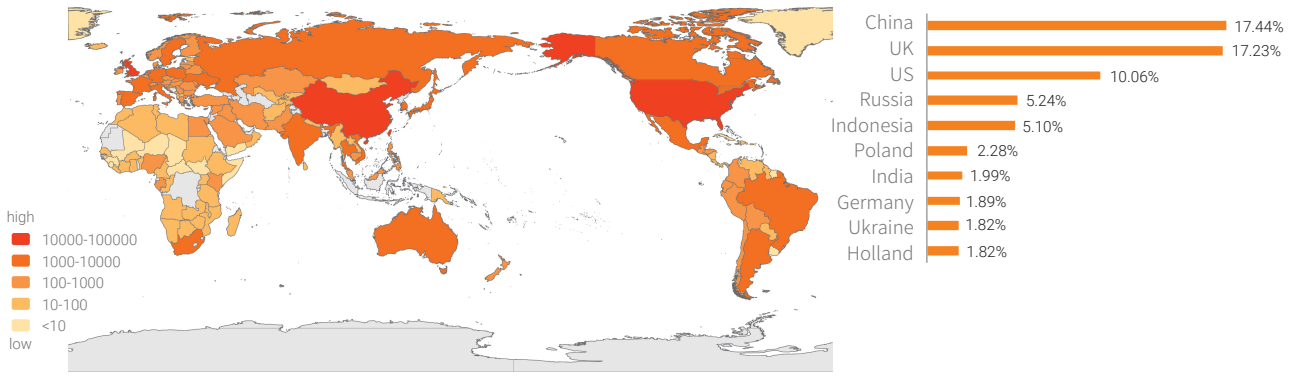


Figure 3-23 Global distribution of active attack sources and proportions of such sources in top countries

Source: NTI and Cloud DPS

3.5.3 "Recidivist" Attack Sources

In 2019, 7% of recidivists[5] were responsible for 78% of DDoS attacks. Obviously, recidivists are too menacing to overlook.

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

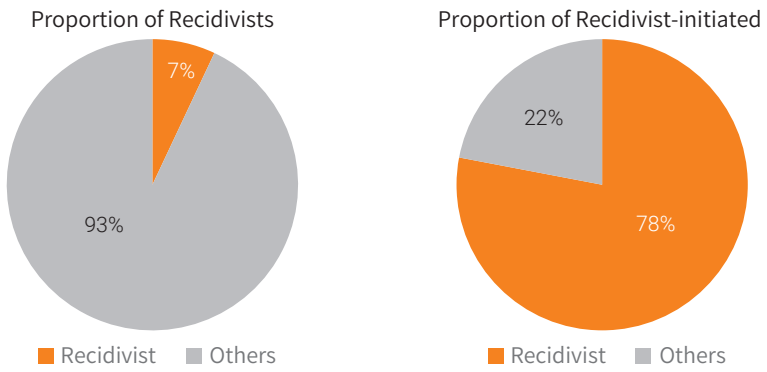


Figure 3-24 Proportion of recidivists and that of recidivist-initiated attacks

Source: NTI and Cloud DPS

3.5.4 Anomalous Behavior

Compared with 2018, attack resources used in DDoS attacks were involved in more types of activity in 2019. Of those resources, 39% had engaged in several types (up to 8) of anomalous activity in 2019.

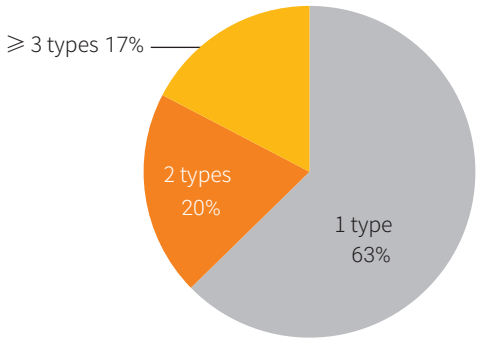


Figure 3-25 Distribution of DDoS recidivists by the number of behavior types

Source: NTI and Cloud DPS

According to proportions of DDoS recidivists' behavior types shown in the following figure, 15.43% of attack sources were controlled by botnets; 7.99% were found in spamming; 58.61% were marked by NTI as to have repeatedly conducted DDoS attacks because they contained vulnerabilities that could be remotely controlled and were left unfixed for a long time, or because they had the reflection capability.

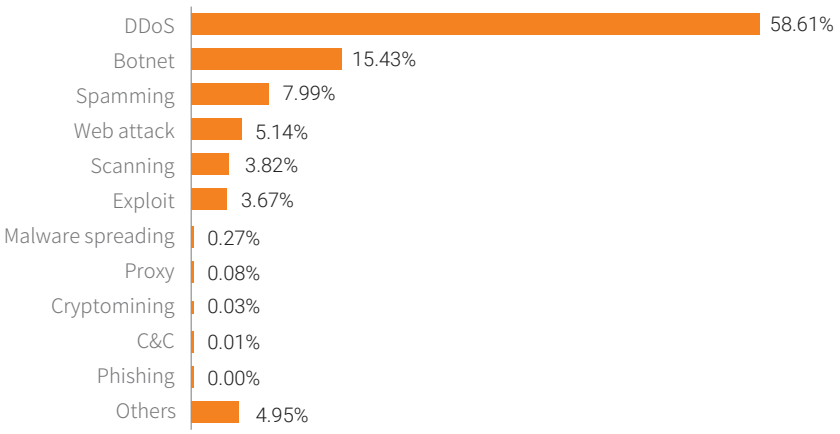


Figure 3-26 Proportions of DDoS recidivists' behavior types

Source: NTI and Cloud DPS

3.5.5 Analysis of Attack Group Behaviors

The previous analysis finds that 7% of DDoS recidivists were responsible for 78% of attack events. However, DDoS attacks are usually launched collaboratively from multiple sources. That is to say, several groups of DDoS recidivists often work together to initiate attacks. Such groups are collectively referred to as an "IP gang". In this report, through analysis of DDoS attack data collected by NSFOCUS in 2019, we have identified multiple IP gangs and done a systematic research on their behavior.

The principle behind our research method is that IP addresses with similar historical attack behavior will be assigned to an IP gang. The behavior similarity is reflected in the following aspects:

1. Behavior similarity in a short time: hitting the same target again and again using the same attack means at the same time.
2. Behavior similarity in the long run: hitting the same target repeatedly using the same attack means in different periods.

In this section, we make a statistical analysis of behavior of IP gangs, profile major ones, and find that IP gangs have the following characteristics:

1. Of recidivists carrying out activities as IP gangs, 17% are IoT devices. This means that IoT devices found in DDoS attacks as attack sources remain active for a long period of time and a large proportion are identified as recidivists. Besides, such devices tend to possess characteristics of gangs performing attacks.
2. For the largest gang with the most attack sources, IoT devices account for 31%, of which 64% are routers (94% from MikroTik).
3. The second largest gang in terms of attack source quantity includes 23,000 recidivists and produces the largest attack traffic. For the recidivists, the most notable characteristic is that they are skilled in the use of volumetric SYN flood attacks as 99.54% of them have resorted to this kind of attack according to historical attack records. For attacks launched in 2019, the peak attack traffic stands at above 100 Gbps for 60 days, with the maximum hitting 780 Gbps.

3.5.5.1 Attack Gang Size

Gang Size

Figure 3-27 shows the distribution of our identified IP gangs by size. Two gangs consist of over 10,000 members and the largest gang has 88,000 members.

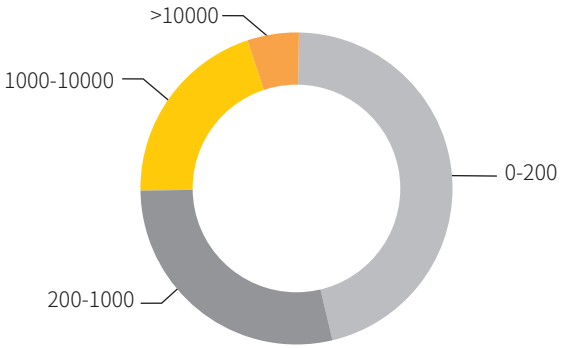


Figure 3-27 Distribution of IP gangs by size (each section indicates a specific size range)

Source: NTI and Cloud DPS

Total Attack Traffic

Figure 3-28 shows the distribution of IP gangs in terms of traffic generated by all members of a gang. As for the total attack traffic, a big gap seemingly existed in different gangs. However, most gangs produced a total of more than 50 TB, with the largest total traffic of one gang hitting 1500 TB.

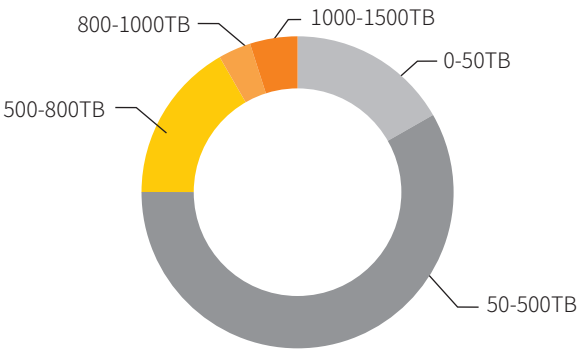


Figure 3-28 Distribution of IP gangs by total attack traffic

Source: NTI and Cloud DPS

3.5.5.2 Largest Gang by the Number of Attack Sources

In 2019, the largest gang with most attack sources was also the most active gang. 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.

Activity Distribution

Figure 3-29 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 will leave (the possible reason is that the system owner has removed the malware and fixed the security vulnerability exploited by the attack controller for system intrusion) while new members will join the gang (new systems are infected with malware and become botnet members).

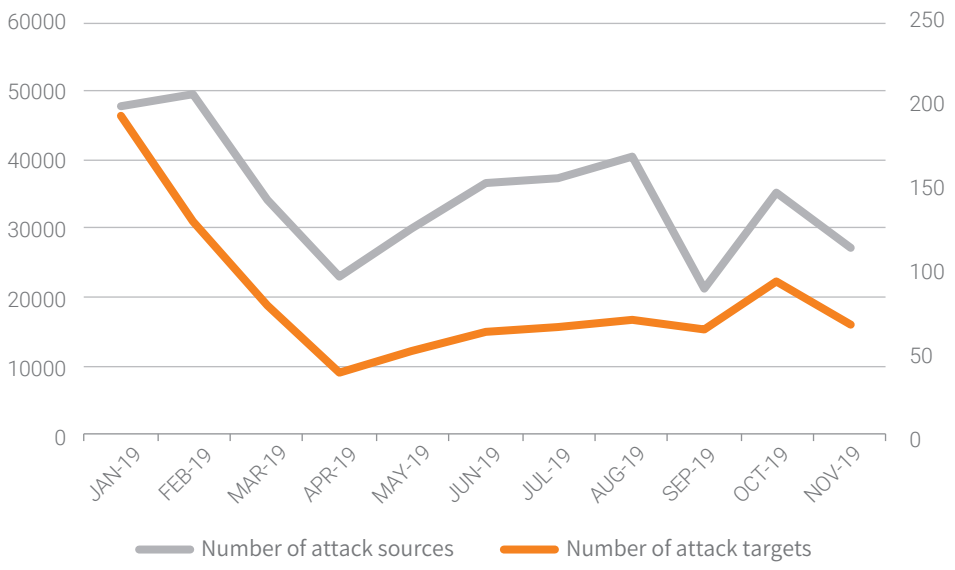


Figure 3-29 Monthly quantity trend of attack sources and attack targets of the largest gang

Source: NTI and Cloud DPS

As shown in Figure 3-30, 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.

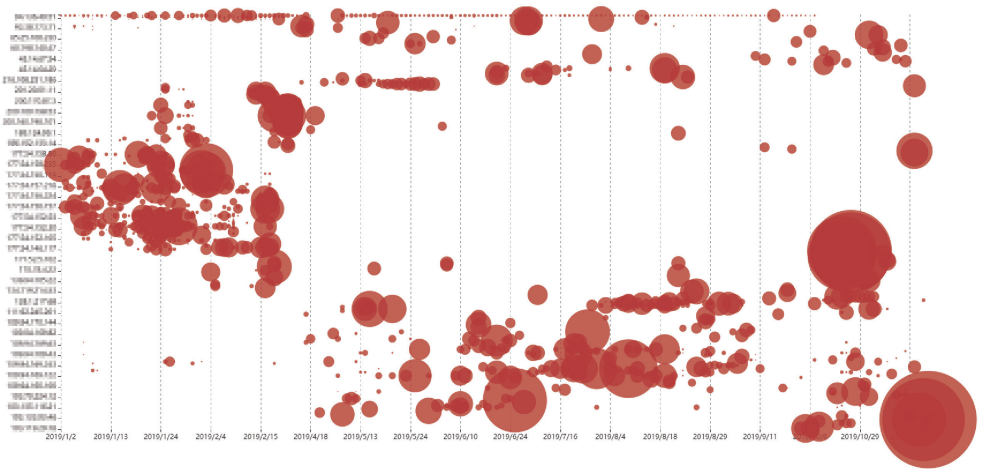


Figure 3-30 Activity distribution of the largest gang

Source: NTI and Cloud DPS

Attack Type Distribution

Figure 3-31 shows the attack type distribution of the largest gang. We can see that this gang mainly resorts to SYN flood and UDP flood attacks.

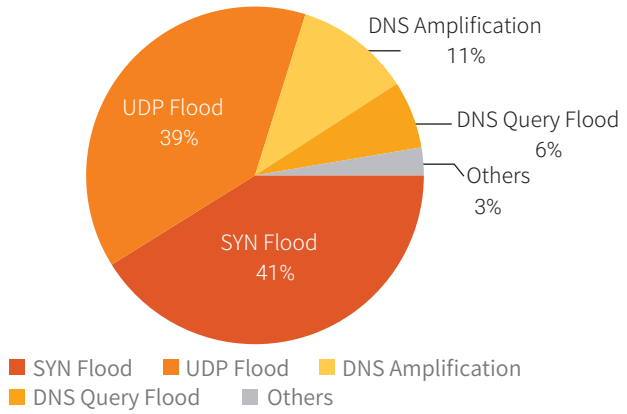


Figure 3-31 Attack type distribution of the largest gang

Source: NTI and Cloud DPS

Distribution of Attack Sources

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.

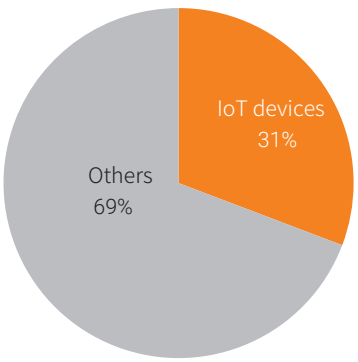


Figure 3-32 Attack type distribution of the largest gang

Source: NTI and Cloud DPS

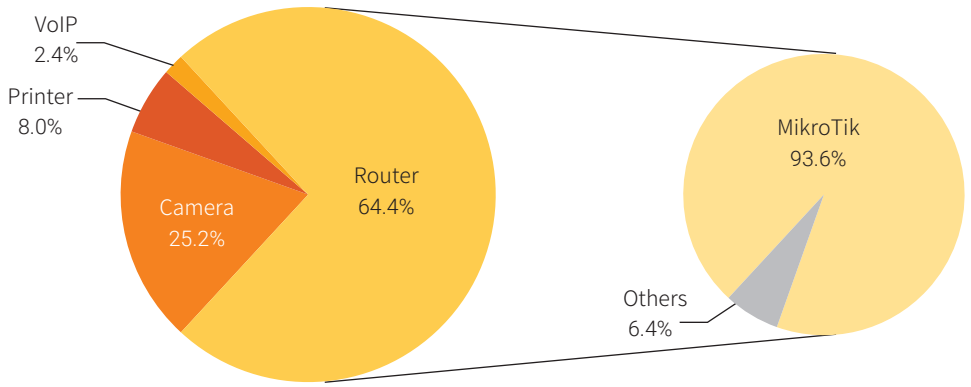


Figure 3-33 IoT device type distribution of the largest gang

Source: NTI and Cloud DPS

Figure 3-34 shows the distribution of attack sources by active duration, with 47% of attack sources remaining active for more than half a year. Obviously, members in this gang are rather active.

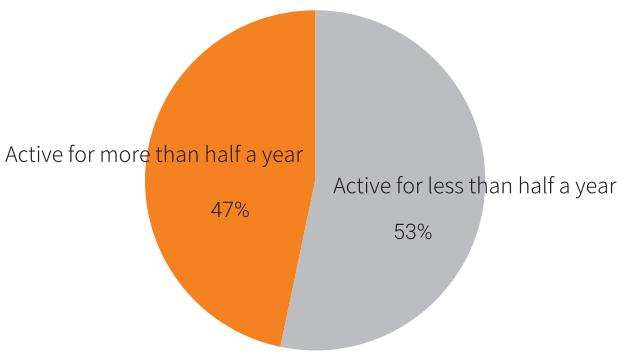


Figure 3-34 Distribution of attacks sources in the largest gang by active duration

Source: NSFOCUS ATM, Cloud DPS, and NTI

3.5.5.3 Second Largest Gang by the Number of Attack Sources

The second largest gang in terms of the number of attack sources generates the largest traffic. This gang has 23,000 recidivists and favors volumetric SYN flood attacks. According to historical attack records, 99.54% of recidivists have resorted to this kind of attack. For attacks launched in

2019, the peak attack traffic stands at above 100 Gbps for 60 days, with the maximum hitting 780 Gbps.

Activity Distribution

Figure 3-35 shows the monthly quantity trend of attack sources and attack targets of this gang. We can see that this gang remains active from January to October, having more attack sources in January, April, May, and June. On average, 6000 active attack sources launch attacks against seven targets each month.

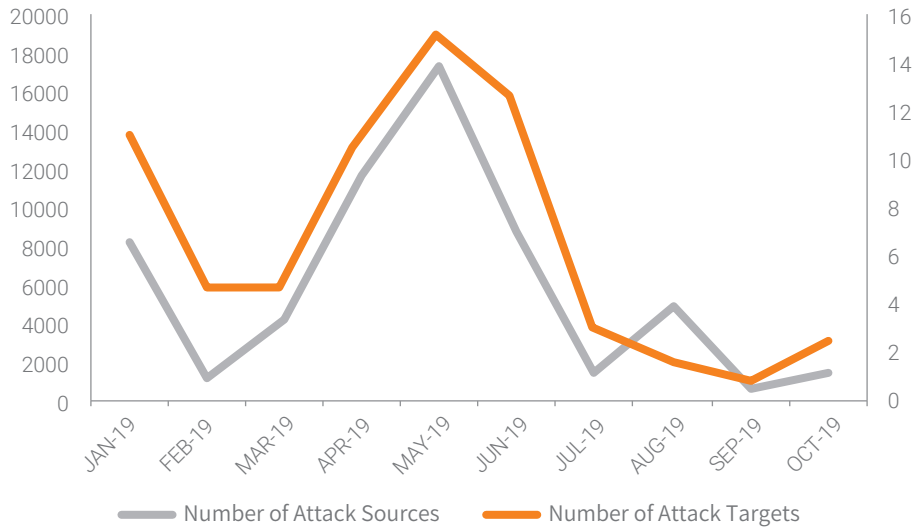


Figure 3-35 Monthly quantity trend of attack sources and attack targets of the second largest gang

Source: NTI and Cloud DPS

As shown in Figure 3-36, 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 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.

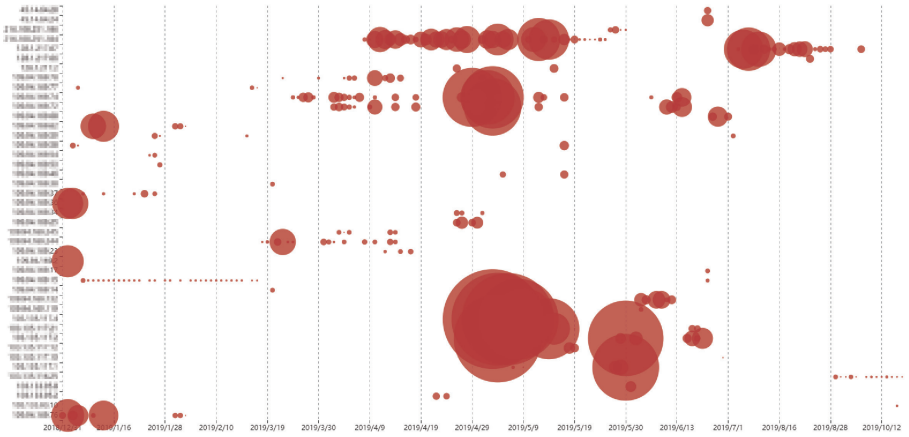


Figure 3-36 Activity distribution of the second largest gang

Source: NTI and Cloud DPS

Attack Type Distribution

Figure 3-37 shows the attack type distribution of the second largest gang. We can see that this gang mainly resorts to SYN flood attacks.

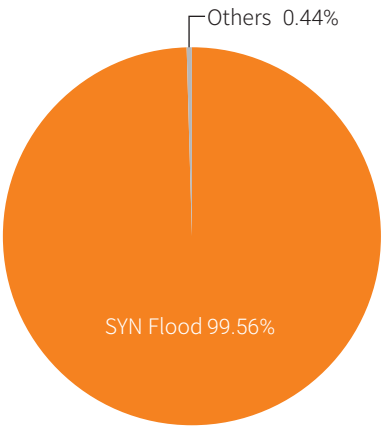


Figure 3-37 Attack type distribution of the second largest gang

Source: NTI and Cloud DPS

Peak Attack Traffic

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 3-38, 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. The peak traffic is a reflection of the gang's control of attack resources and attack ability.

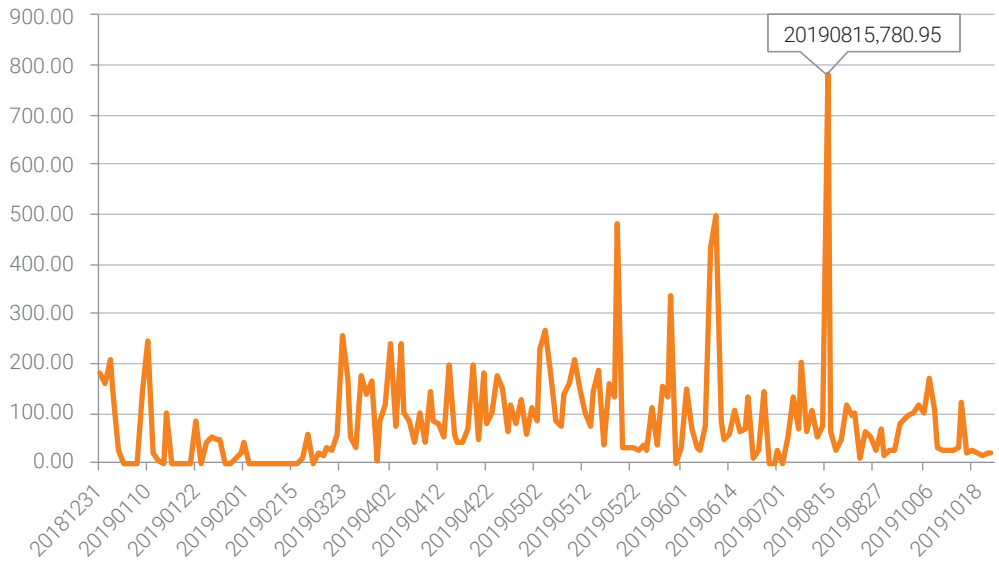


Figure 3-38 Peak traffic trend of the second largest attack source

Source: NTI and Cloud DPS

3.6 Analysis of IoT Attack Resources

3.6.1 Participation of IoT Devices in DDoS Attacks

According to our observation, there were a total of more than 1,280,000 IP addresses of abnormal IoT devices around the world, accounting for 2.1% of all global IoT devices. Of all those abnormal

IoT devices, 170,000 were involved in DDoS attacks, making up 13.08% of the total.

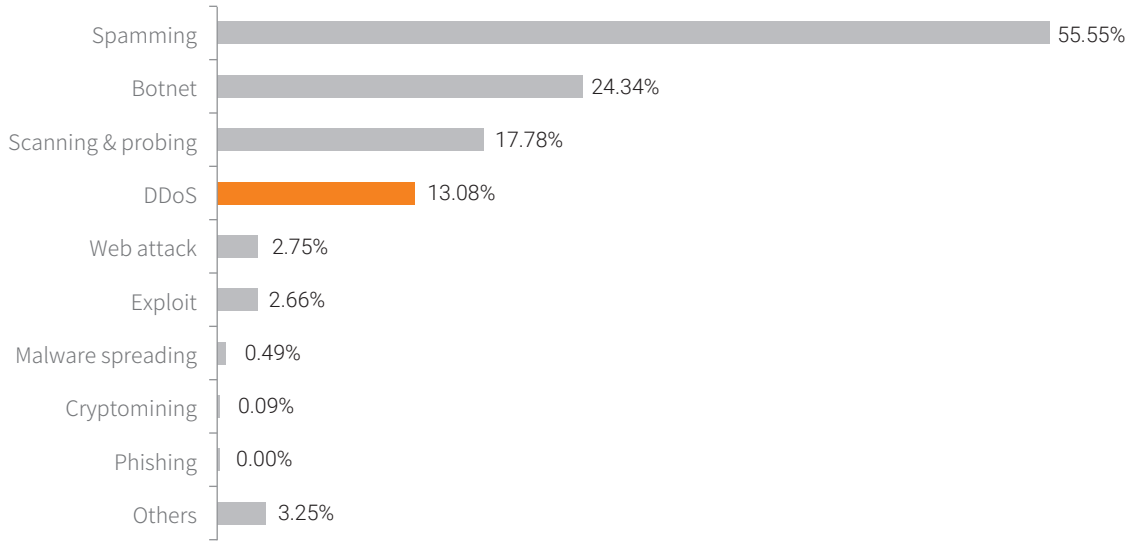


Figure 3-39 Distribution of abnormal IoT devices by behavior[6]

3.6.2 Geographical Distribution of IoT Devices Involved in DDoS Attacks

By analyzing the global distribution of IoT devices involved in DDoS attacks, we found that most of such devices were located in China, mainly because the data collection probes of IoT devices deployed in China were more than those deployed overseas. China, Britain, Russia, the USA, and Vietnam were top 5 countries housing the most devices.

6 The sum of proportions in this figure exceeds 100% because certain devices are engaged in more than one type of abnormal behavior.

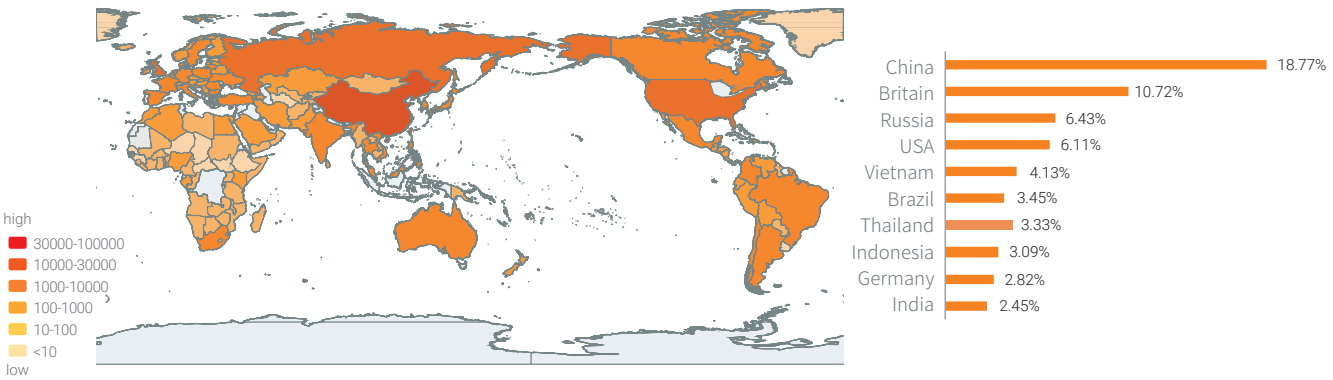


Figure 3-40 Global distribution of IoT devices involved in DDoS attacks

3.6.3 Distribution of IoT Devices Involved in DDoS Attacks by Type

Routers and cameras are the major sources of IoT device-based attacks. Regarding device types, the main types of IoT devices involved in DDoS attacks were routers and cameras, accounting for about 90%. This is consistent with the type distribution of IoT devices.

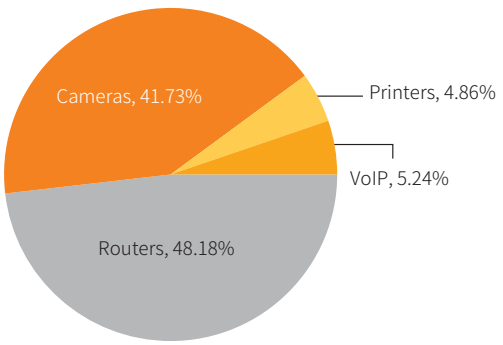


Figure 3-41 Distribution of IoT devices involved in DDoS attacks by type

3.7 DDoS Botnets

3.7.1 Overview

In 2019, NSFOCUS Security Labs detected over 400,000 DDoS attacks launched via botnets, a sharp increase compared with 2018 (8323 DDoS attacks). According to our observation, the botnets running on IoT devices were mainly Mirai and Gafgyt families. These two families were exploited to launch over 60% of DDoS attacks in the first half of 2019. The following figure shows the proportions of high-risk commands observed by NSFOCUS Security Labs in 2018 and 2019.

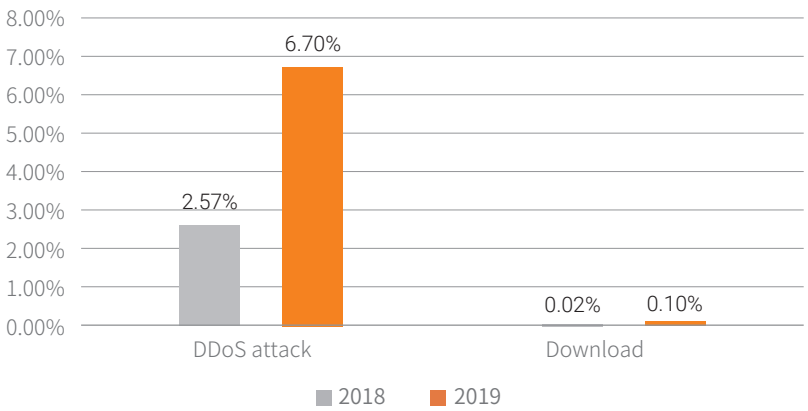


Figure 3-42 Proportions of high-risk commands in 2018 and 2019

Compared with 2018, the attacks observed by NSFOCUS Security Labs increased significantly and the number of download directives saw a five-fold increase. The directives of downloading high-risk commands increased more rapidly than DDoS attack directives. This indicates that botnets not only continue to improve their DDoS attack capabilities, but also begin to develop a new trend of propagating other malware.

In terms of DDoS attack types, compared with 2018, UDP flood, TCP flood, and SYN flood attacks still dominated DDoS attacks in number.

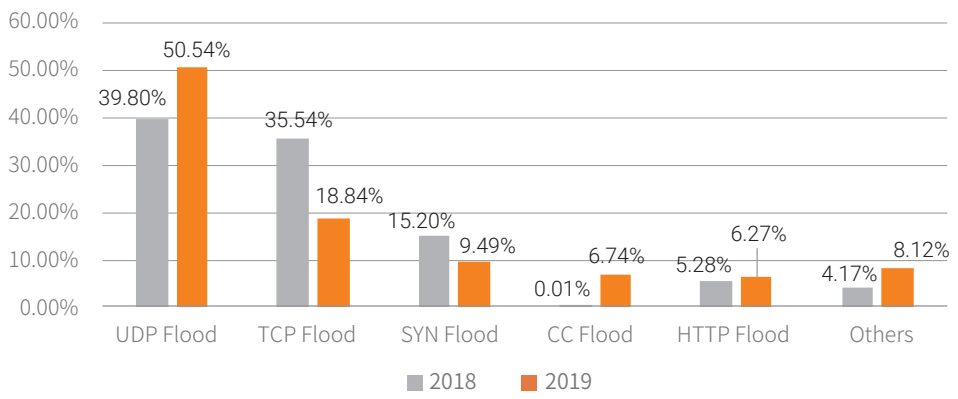


Figure 3-43 Comparison of DDoS attack types

The following figure shows the proportions of current attacks by type in 2019. Compared with 2018, UDP attacks increased sharply, while TCP attacks decreased slightly. One of the reasons why TCP attacks decreased is that CC flood attacks surfaced as a new type of attacks.

Most DDoS attacks were launched via botnets. The following figure shows the activity of botnet families monitored by NSFOCUS Security Labs in 2019.

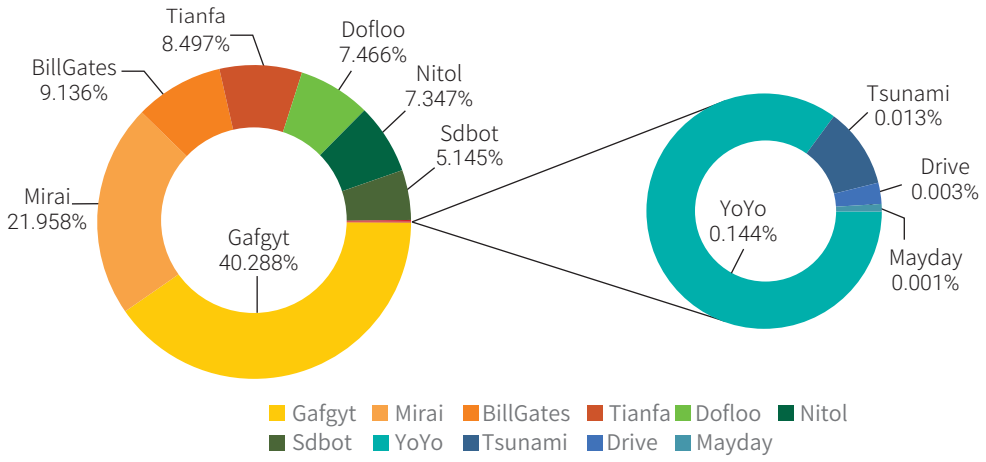


Figure 3-44 Activity of botnet families

In 2019, botnet families mainly targeted IoT platforms, with Gafgyt and Mirai taking the largest proportion. Though the BillGates family was exploited to launch DDoS attacks most frequently in 2018, the number of such attacks declined greatly in 2019. We believe that in a scenario where the BaaS model becomes increasingly mature, attackers prefer to exploit open-source DDoS families for automatic deployment.

According to the monitoring of NSFOCUS Security Labs, the propagation methods used by botnets during the expansion were upgraded from 2018. The exploit payload of IoT botnet families in 2019 shared similarities with that in 2018, mainly targeting smart IoT devices by exploiting CVE-2017-17215 and CVE-2014-8361 vulnerabilities.

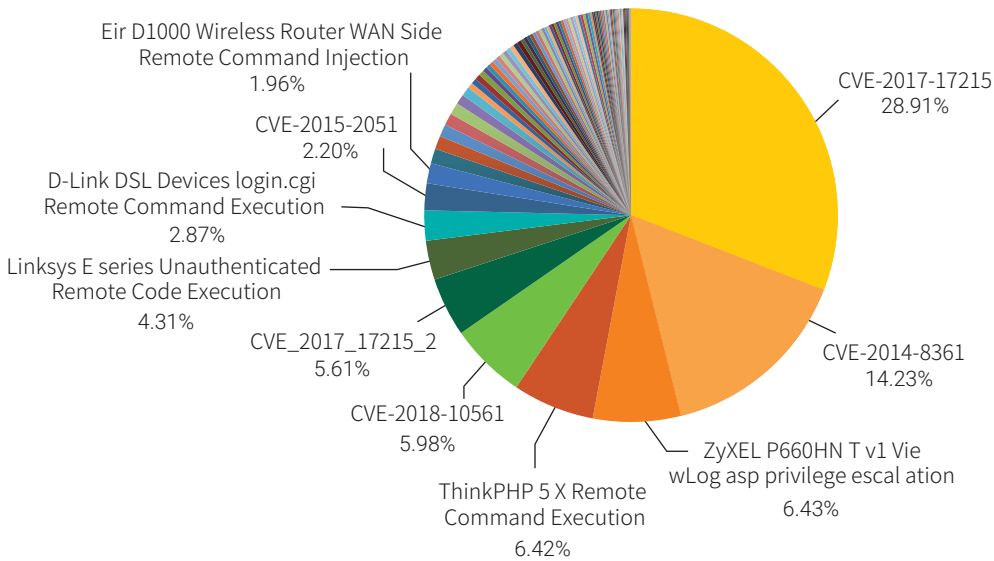


Figure 3-45 Distribution of exploit payloads

At the same time, the number of IoT family-based exploits hit the three-digit mark for the first time, reaching 103, with a broad chronological span.

Windows botnet families tend to spread by exploiting weak passwords, phishing documents, and CVE vulnerabilities. Phishing document-based spreading can be subdivided into macro viruses-

based spreading and Office vulnerabilities-based spreading. The following figure shows their respective proportions.

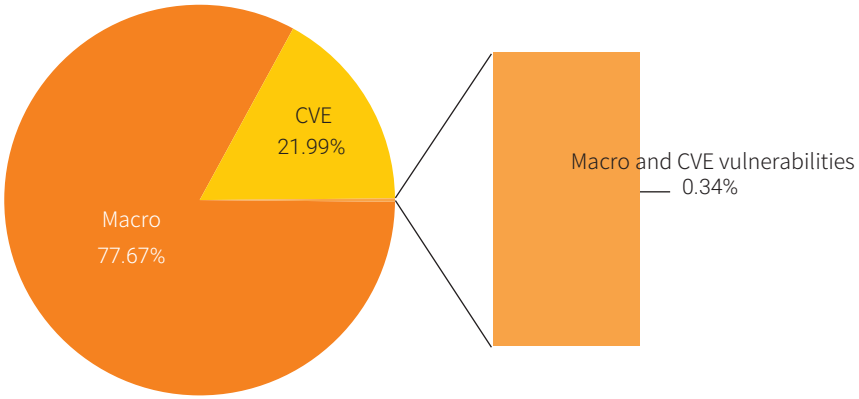


Figure 3-46 Proportions of Office vulnerabilities and macro viruses

As a representative of vulnerabilities that spread via system-level CVE vulnerabilities, the EternalBlue vulnerability is widely found in the spreading process of cryptominers and ransomware.

The following sections dwell upon the most active DDoS families, Gafgyt and Mirai.

3.7.2 Active Families

3.7.2.1 Gafgyt

As one of the largest IoT DDoS families, Gafgyt compromises such devices as routers and cameras by means of password cracking and exploits to receive C&C commands and launch DDoS attacks.

In 2019, the Gafgyt family continued to be active, mainly targeting North America, Europe, and Australia. The number of Gafgyt-based malware increased fourfold compared with 2018 and the average daily increase of C&C attacks reached 34.5%. Compared with 2018, the number of DDoS attack directives increased by 175%, most of which were UDP flood attacks targeting ports 80 and 443 for HTTP services and ports 3074, 300000, 30100, and 32000 for gaming services.

C&C servers of the Gafgyt family are mainly deployed on virtual private servers (VPSs). In 2019, the Gafgyt family used servers from more than 90 different VPS providers. According to the statistics, the cheaper a server the more popular it is with attackers.

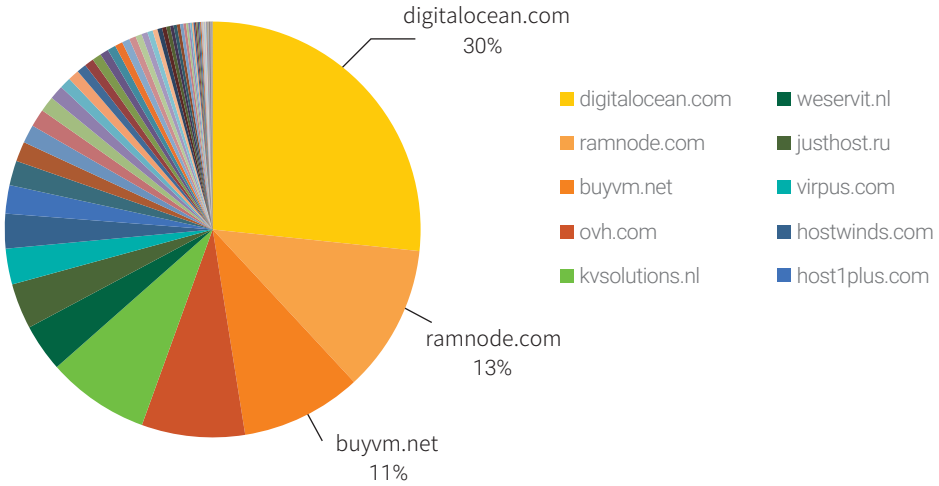


Figure 3-47 Distribution of cloud service providers of Gafgyt C&C servers

Attackers who exploit Gafgyt keep foraging vulnerabilities existing in various devices. According to NSFOCUS Security Labs, the exploit payload targeting Huawei HG532 router and ZyXEL P660HN router was most frequently used. A large number of Gafgyt programs continuously scan routers for vulnerabilities after being executed. Once a vulnerable device is within the scanning scope, it will be compromised immediately and become a new scanning node. In this way, the size of Gafgyt nodes keeps expanding. This is the biggest headache brought by IoT devices.

Furthermore, Gafgyt also uses other scripts for launching DDoS attacks and executing other commands, so as to make up for the inefficiency of DDoS directives and bypass DDoS protection policies of certain cloud service providers.

3.7.2.2 Mirai

At present, Mirai is one of the biggest IoT DDoS families. In 2019, NSFOCUS Security Labs have tracked as many as 1660 C&C addresses, nearly half of which were deployed on the cloud/VPS hosts (see the following figure), and captured over 10,000 pieces of malware throughout the year (excluding cross-compiled and repeated types).

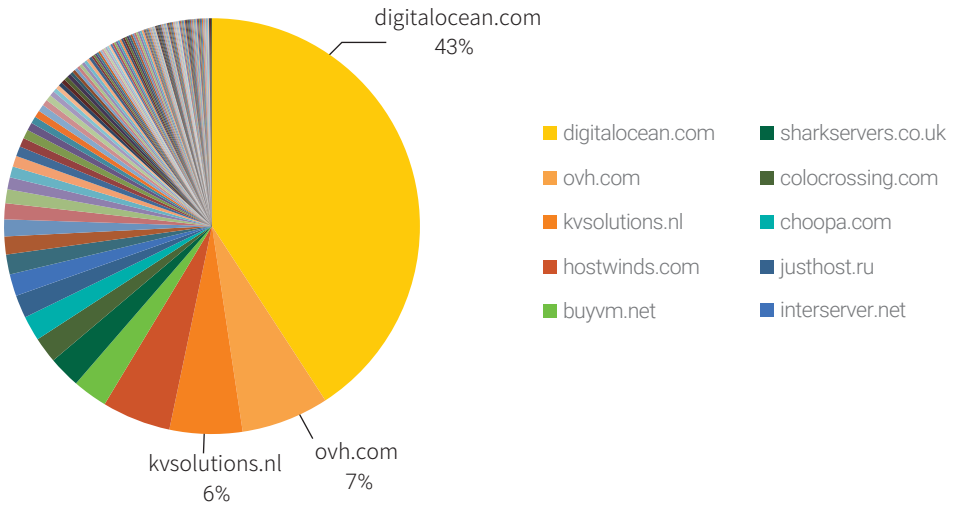


Figure 3-48 Distribution of cloud providers of Mirai C&C servers

In 2019, Mirai variants kept increasing and their exploits exceeded 40.

In addition, Mirai variants continuously updated their DDoS attack arsenals so as to be able to launch more diverse attacks such as TCP reset attacks, small UDP packet attacks, abnormal TCP packet attacks, HTTP POST attacks, HTTP GET attacks, and DNS reflection attacks.

Another new characteristic of Mirai variants in 2019 is that Tor was used as a proxy for C&C communication. Before connecting to the C&C server, zombies first connect to the proxy server. They will not connect to the C&C server on the dark web for receiving directives until they receive a message confirming the successful connection.

4

Looking Forward

Looking Forward

Most security experts agree that DDoS attacks are here to stay and they're not going away any time soon. With 5G technology becomes more widely available, anyone with a 5G phone can easily launch a DDoS attack greater than 1G of bandwidth. Network security practitioners need to consider adding DDoS protection to the edge network to mitigate against 5G based DDoS attacks.

Gartner analysts project that demand for security-as-a-service, referred to as secure access service edge (SASE), will grow significantly in the next five years, estimating that by 2024, a minimum of 40% of companies will have plans to adopt SASE. You should make plans to beef up security protection for cloud edge.

Analysis finds that 7% of DDoS recidivists were responsible for 78% of attack events. Network security practitioners should monitor IP chain-gangs and take proactive measures.

With the expected growth of 5G based DDoS attacks and Gartner's recommendation for SASE, network security practitioners should consider hybrid DDoS solution as the standard DDoS solution. With hybrid solution, the on-premises solution allow network administrators to develop security polices to protection edge network with more granular control and lower latency while leveraging cloud based DDoS protection for less frequent but larger scale attacks.

2019 DDoS Attack Landscape

NSFOCUS