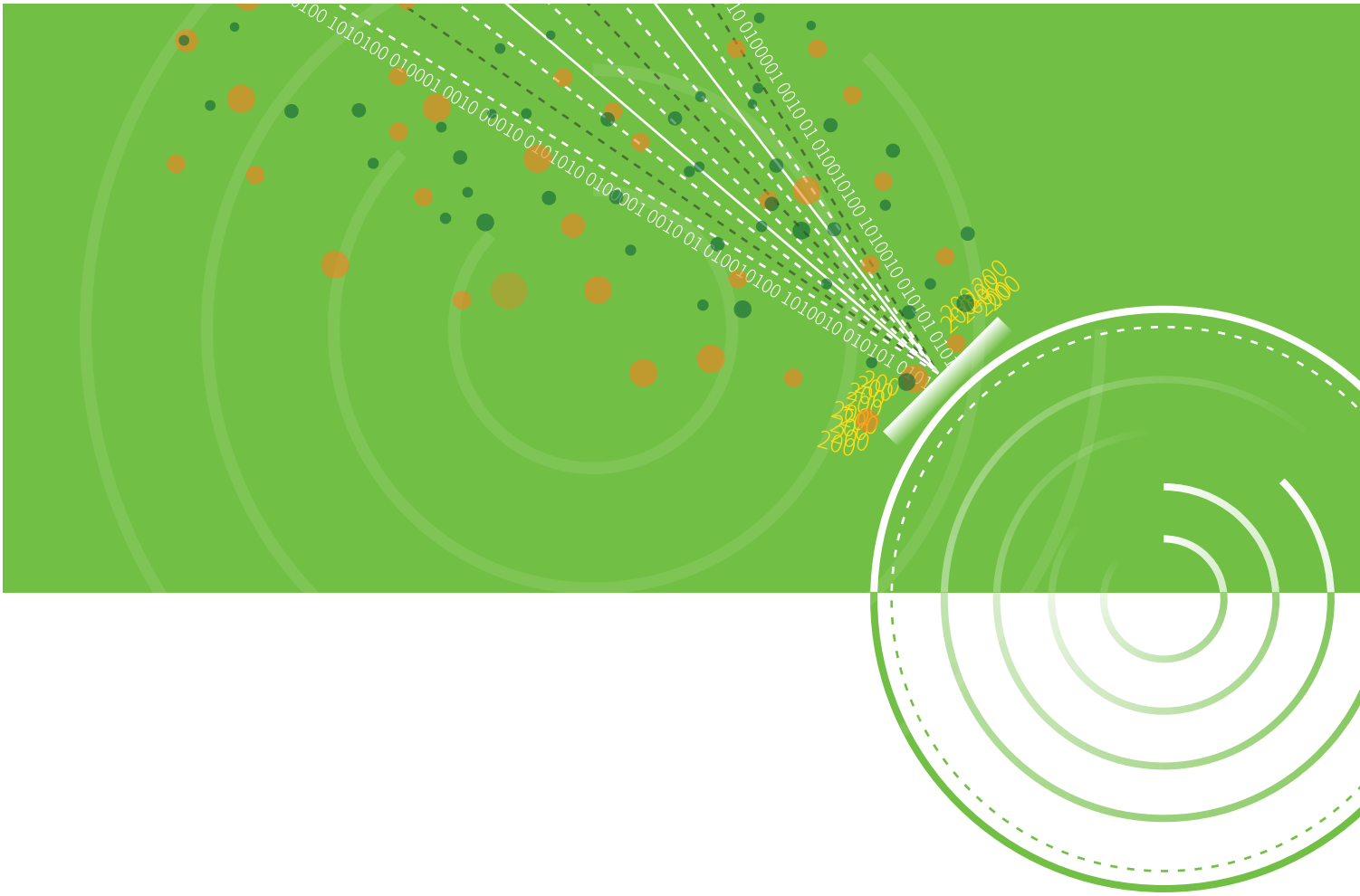
中国电信·云堤 CHINA TELECOM NSFOCUS

2018 DDoS Attack Landscape



About DamDDoS

Since 2008, China Telecom has been focusing on constructing capabilities of defending against DDoS attacks on the network, and formed an integrated defense system covering 31 provinces in China and major POPs in Asia Pacific, Europe, and North America.

In 2014, for the first time in the industry, China Telecom systematically put forward the framework of an open platform for the intensive security capability of carrier-class networks, with DamDDoS as a unified brand for external services.

In the past few years, DamDDoS has been committed to building efficient, reliable, accurate, and open capabilities of defense against DDoS attacks, while providing carrier-class DDoS attack defense services to government and enterprise customers. Currently, it covers various sectors such as the Internet, finance, energy, manufacturing, and government.

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, a member of 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.

CONTENTS

CONTENTS

1

Executive Summary

Executive Summary

2018 witnessed transformations in every corner of both cyberspace and the real world driven by the every quickening growth of the Internet as well as the implementation of revolutionary and evolutionary technologies related to cloud computing, big data, artificial intelligence (AI), Internet of things (IoT), and Industry 4.0.[1] Every one of these exerted a continuous and extensive influence upon people's livelihood, business development, and national strengths. Amid fast technological innovations, the threats facing netizens and cyberspace are also changing and escalating.

Technological and industrial environments are changing, leading to much different battlefields between the offensive and defensive than before. Cyberattack methods and their intensity keep evolving and upgrading, making it easier to launch DDoS attacks, which have never stopped since they made their debut.

In February 2018, an IPv6 DDoS attack targeting DNS servers was spotted, making it the first documented attack of its type. According to Neustar, a DNS service provider, hackers are deploying new methods for IPv6 attacks, not simply replicating IPv4 attacks using IPv6 protocols.[2] In March 2018, GitHub, a well-known code hosting website, was hit by a DDoS attack that peaked at 1.35 Tbps. It was reported that the attack group behind this attack used artificial intelligence (AI) and machine learning algorithms to automatically amplify the amount of traffic based on the distributed memory caching system Memcached. At the time of writing, the largest DDoS attack based on Memcached was recorded at 1.7 Tbps.[3]

The effectiveness of attack methods and the convenience of profit-making are major contributors to the long-lived DDoS attacks, which, together with cryptomining, have topped the list of attacks most favored by attackers in the past two years. The Cybersecurity Law of the People's Republic of China came into force in 2017 and then the second half of the year saw a sharp rise in the value of cryptocurrency represented by Bitcoin. In this context, prime botnet resources available in the black market began to be switched from comparatively costly DDoS attacks to cost-efficient cryptomining activities. The

1 https://en.wikipedia.org/wiki/Industry_4.0
2 https://www.scmagazineuk.com/first-true-native-ipv6-ddos-attack-spotted-wild/article/1473177
3 https://www.wired.com/story/github-ddos-memcached/

fluctuation of Bitcoin prices has a direct bearing on DDoS attack traffic. In 2018, we found that attackers were more inclined to launch DDoS attacks when the short-term benefits from cryptomining activities declined. Profits are the permanent pursuit of attackers, who always take DDoS as a handy weapon. Defenders cannot afford to overlook such a fact.

Chapter 2 compares DDoS attack situations in 2017 and 2018 and sums up major characteristics of DDoS attacks in 2018. Chapter 3 presents DDoS changes seen by NSFOCUS in 2018 reflected in the attack traffic, frequency, and size through a multidimensional analysis of attack sources, attack types, attack durations, geographic distribution of attacks, participation of IoT devices, and distribution of attack targets by industry, in a bid to help organizations and agencies improve their network defense techniques and systems.

2

Overview of DDoS Attacks in 2018

2.1

2018 VS 2017

Fall — The total number of DDoS attacks seen by NSFOCUS in 2018 reached 148,000, down 28.4% from 2017.

Stable — The total volume of DDoS attack traffic seen by NSFOCUS in 2018 reached 643,100 TB, on a par with 2017.

Raise — The average peak traffic of individual DDoS attacks seen by NSFOCUS in 2018 increased 204% from 2017 to 42.8 Gbps.

Stable — The maximum peak traffic in a single DDoS attack in 2018 reached 1.4 Tbps, on a par with 2017.

Fall — The average attack duration in 2018 seen by NSFOCUS decreased 17% from 2017 to 42 minutes.

2.2

Key Findings

Finding1 In 2018, DDoS attacks kept expanding in size as DDoS-as-a-Service experienced a fast growth.

Finding2 DDoS attackers were obviously profit-driven and sensitive to regulatory policies and national governance measures.

Finding3 The number of reflection attacks decreased and those DDoS attacks using mixed methods called for more attention.

Finding4 IoT-related threats were looming large as a result of medium and high vulnerabilities in a variety of IoT devices that could be exploited by malware.

Finding5 Most DDoS attacks took place during busier hours of a day to maximize the attack effect.

Finding6 Cloud services/IDCs, gaming, and e-commerce were top 3 industries targeted by attackers, with cut-throat competition as the major driver.

Finding7 Botnet command and control (C&C) servers were mainly distributed in the USA and China.

Finding8 China still ranked No. 1 in terms of both total attack sources and attack targets.

3

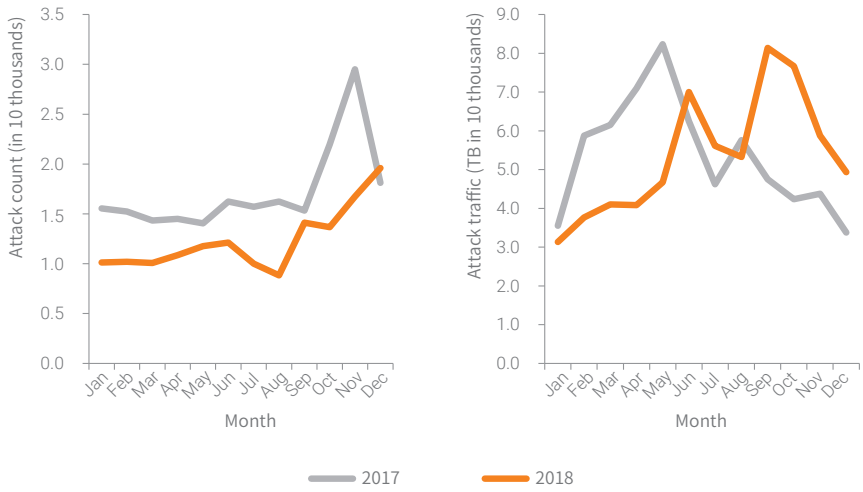
Analysis of DDoS Attacks in 2018

3.1 DDoS Attack Count and Peak Size

3.1.1 Attack Count and Traffic

In 2018, we observed 148,000 DDoS attacks (down 28.4% from 2017), which generated a total of 643,100 TB of traffic, about the same level as in 2017. DDoS attacks keep expanding in size year by year as large and medium-scale attacks are on the rise, as shown in section 3.1 "Distribution of Peak Sizes."

Figure 3.1 Monthly attack count and attack traffic in 2018 (China Telecom DamDDoS)

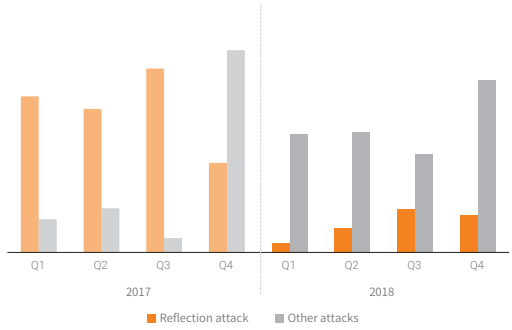


Source: DamDDoS

In 2018, the number of DDoS attacks dropped significantly, driven by effective protections against reflection attacks. Since the beginning of 2018, the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), in cooperation with carriers and cloud service providers around the country, carried out a special campaign against attack resources in China using techniques including identifying bogus source IP addresses and making reflection attack sources known to the public. These governance measures have effectively reduced the success rate of reflection attacks, forcing attackers to resort to other means. According to statistics, in 2018, the number of

reflection attacks decreased 80%, but that of other attacks increased 73%. As a result, reflection attacks accounted for only 3% of all DDoS attacks.

Figure 3.2 Reflection attacks vs. other attacks in 2017 and 2018 (China Telecom DamDDoS & NSFOCUS ATM)



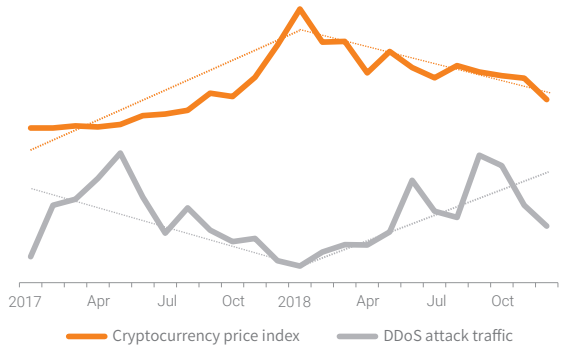
Source: DamDDoS

In the first half of 2018, the number of DDoS attacks increased slowly, but in the second half, the increase accelerated. We believe that the month-over-month increase in the number of DDoS attacks was linked with the fall of cryptocurrency prices. In the 2017 DDoS and Web Application Attack Landscape[4], 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 2018, the price of cryptocurrency dropped, leading to decreased profits from cryptomining, which, in turn, made DDoS attacks more attractive and increase month by month.

Comparing the monthly Bitcoin price with the monthly DDoS attack traffic, we get the Pearson correlation coefficient of –0.48, indicating a negative correlation between the two, which corroborates our findings from last year.

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

Figure 3.3 DDoS attack traffic changing with Bitcoin prices (China Telecom DamDDoS)

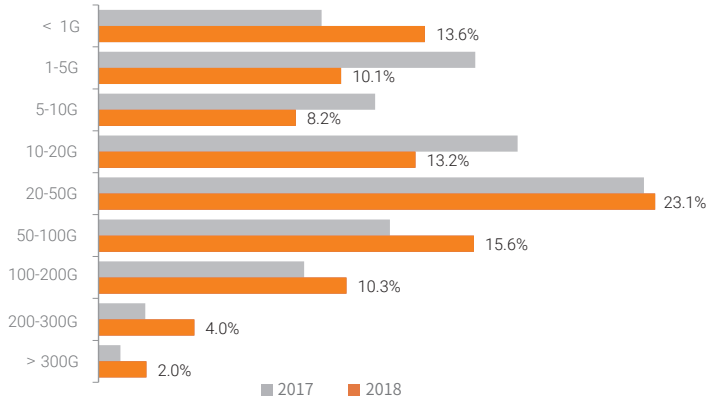


Source: DamDDoS

3.1.2 Distribution of Peak Sizes

The peak sizes of DDoS attack traffic mainly ranged from 20 to 50 Gbps and attacks within this range accounted for 23.1% of all DDoS attacks. Compared with 2017, the year 2018 saw a decrease in small-scale attacks (< 20 Gbps), an increase in medium- and large-scale attacks (20–200 Gbps), and double the super-large attacks (> 200 Gbps).

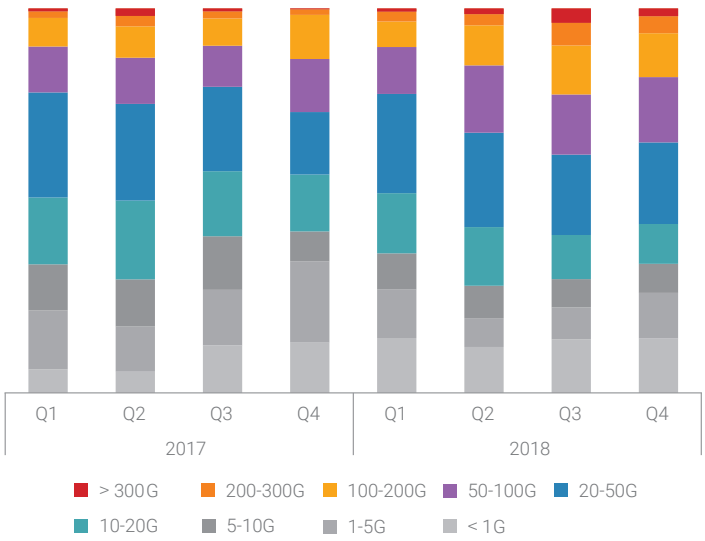
Figure 3.4 Distribution of attacks by peak size 2017 vs 2018 (China Telecom DamDDoS)



Source: DamDDoS

According to quarterly statistics, the number of large DDoS attacks with a peak rate of greater than 100 Gbps steadily increased. From the second quarter, large attacks increased rapidly, especially in the third quarter when large attacks took up 23% of the total attacks.

Figure 3.5 Quarterly counts of DDoS attacks by peak size in 2017 and 2018 (China Telecom DamDDoS)



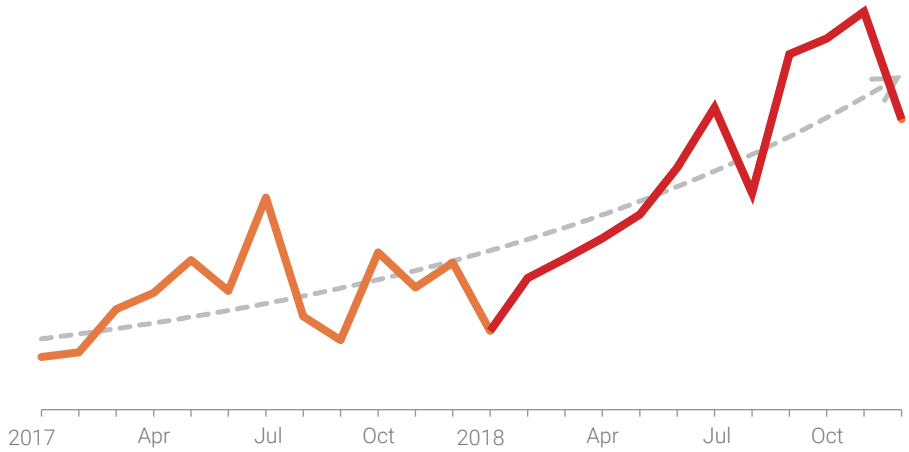
Source: DamDDoS

In recent years, super-large attacks have emerged and constantly grown in the peak size. In March 2018, the well-known code hosting website GitHub was hit by a DDoS attack peaking at 1.35 Tbps. As of the time of writing, the peak traffic rate of DDoS attacks had reached a record high of 1.7 Tbps.[5]

The monthly statistics in the past two years reveal that large attacks with a peak rate of more than 100 Gbps have rapidly increased. This indicates that the scale of attack resources controlled by attackers is expanding and their attack capabilities are constantly upgraded.

5 https://www.wired.com/story/github-ddos-memcached/

Figure 3.6 Number of large attacks (> 100 Gbps) by month (China Telecom DamDDoS)



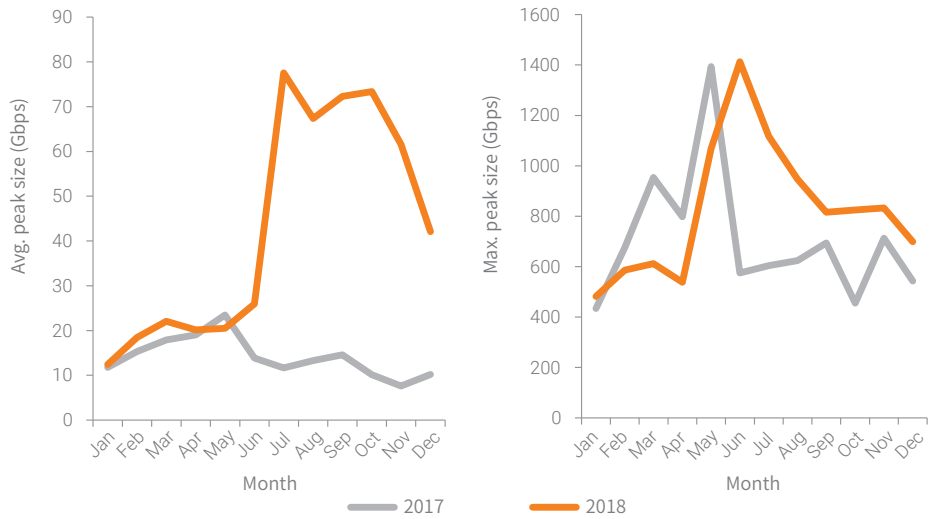
Source: DamDDoS

3.1.3 Maximum and Average Peak Sizes of Individual Attacks

In 2018, the average peak size of DDoS attacks hit 42.8 Gbps, thrice that of 2017 (14.1 Gbps). Peak sizes were especially large in the second half of 2018, reaching 67 Gbps, mainly driven by the widespread improvement of network bandwidths and significant enhancement of DDoS attack capabilities.

As for the maximum peak size, we observed an attack in June 2018 peaking at 1.41 Tbps, on a par with 2017.

Figure 3.7 Average peak sizes and maximum peak 2017 vs 2018 (China Telecom DamDDoS)



Source: DamDDoS

The improved DDoS attack capabilities and the record high of average peak sizes both point to the fact that DDoS attacks are becoming increasingly more damaging. As a matter of fact, most hackers can generate super-large traffic and their capabilities are still growing rapidly, which is becoming a greater challenge for defenders and security governance personnel.

3.2 DDoS Attack Type Analysis

3.2.1 Proportions of Different Attack Types

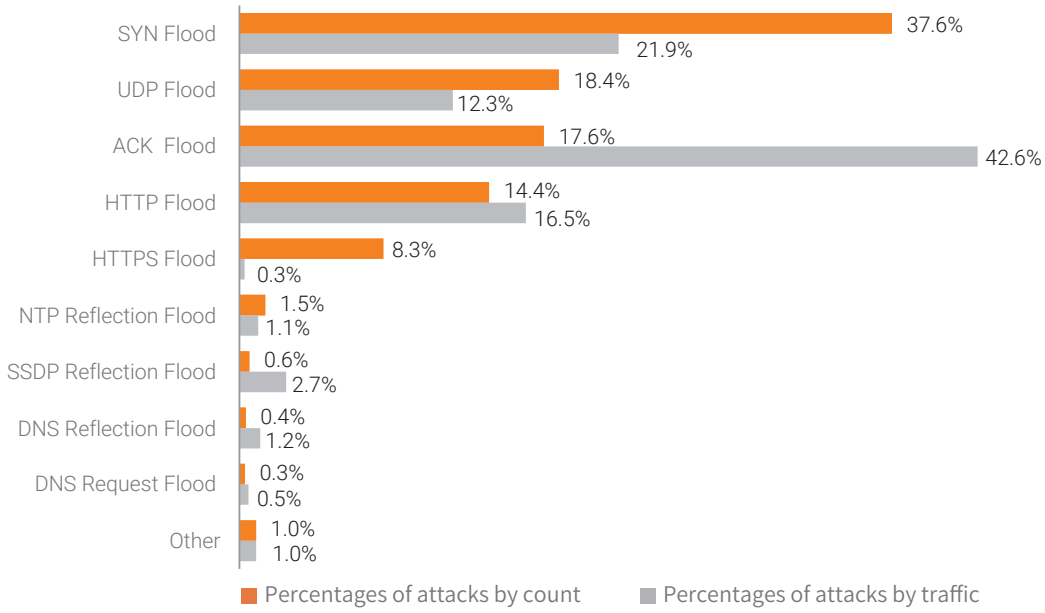
In 2018, the most frequently seen attacks were SYN flood, UDP flood, ACK flood, HTTP flood, and HTTPS flood attacks[6], which altogether accounted for 96% of all DDoS attacks. In contrast, reflection attacks contributed to no more than 3% of attacks. Compared with 2017, the year 2018 witnessed an 80% decrease in the number of reflection attacks, but a 73% increase in other attacks. This is because Chinese authorities took effective measures against reflectors (see section 3.1.1 "Attack Count and

6 Here, we break down multi-vector attacks into respective types

Traffic").

In terms of attack traffic, ACK flood attacks generated 42.6% of the total attack traffic. The likely reason for this is that certain sectors (like gaming) have large quantities of users and sessions as well as long-lived connections, making them easy targets of ACK attacks characterized by large packets.

Figure 3.8 Percentages of different attack types by count and traffic



Source: NSFOCUS ATM

SYN flood attacks still stood out among all types of DDoS attacks. This attack exploits defects in the TCP protocol, where an attacker sends a large number of TCP connection requests to exhaust resources of a target. This exploit method is seldom used independently, but rather used with SYN floods to overwhelm hosts and firewalls that must perform large quantities of calculations to determine whether ACK packets are legitimate. This will deplete resources of the target and at the same time complete a traffic-based attack.

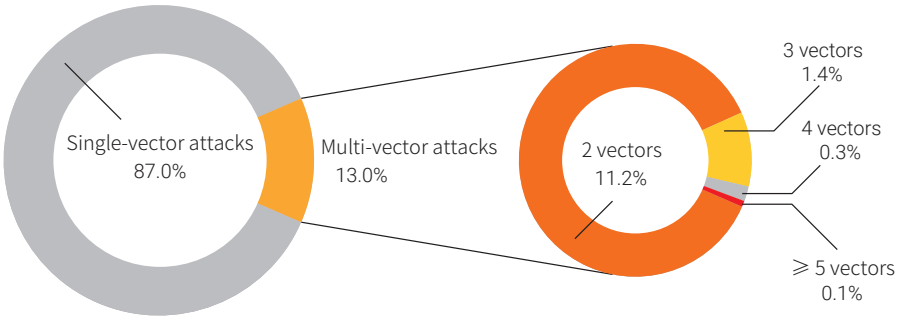
UDP floods are long-lived, traffic-based DDoS attacks. Usually, an attacker floods DNS servers, RADIUS authentication servers, or streaming media servers with a large number of small UDP packets. As a

simple protocol, UDP makes it extremely easy to generate large amounts of traffic as UDP floods do not require setup of connections, thus becoming a most favored attack method.

HTTP floods and HTTPS floods are attacks launched at the application layer against web servers. An attacker conducts this type of attack by simulating a legitimate user accessing websites. This may cause serious chain effects. When a client keeps sending requests while performing frequent database operations, not only will the web frontend respond slowly, but the backend server program will also be indirectly affected. In the worst-case scenario, backend services, such as the database, may stop responding or crash, and even related hosts, such as the log storage server and image server, may be compromised.

Of all DDoS attacks, 13% 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 difficult and costly to effectively analyze, respond to, and mitigate such distributed attacks involving various protocols and leveraging various resources.

Figure 3.9 Distribution of multi-vector attacks



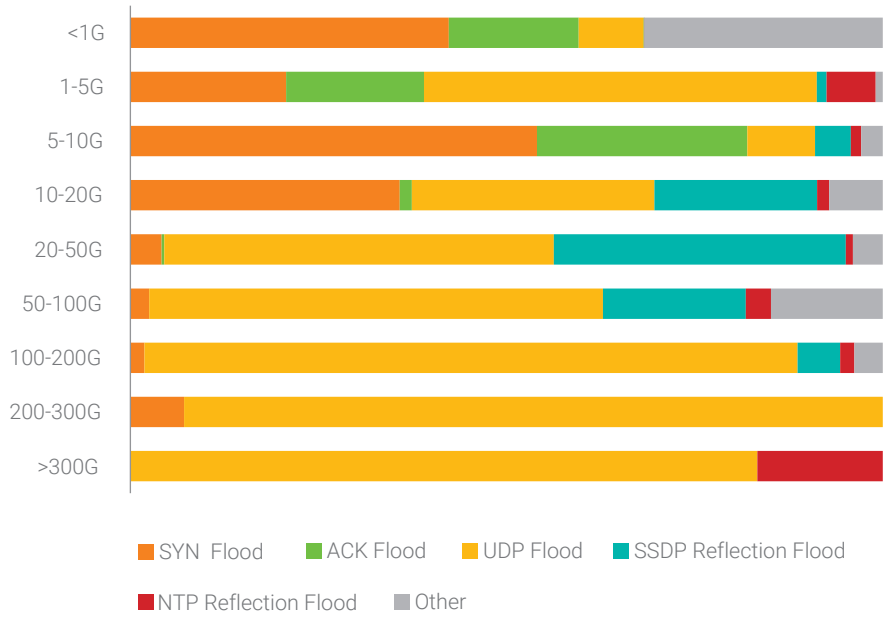
Source: NSFOCUS ATM

3.2.2 Distribution of Attack Types by Consumed Bandwidth

In 2018, DDoS attacks with a peak rate of less than 10 Gbps were mostly conventional attacks like SYN and ACK floods. Attacks ranging from 10 Gbps to 100 Gbps mainly used UDP and SSDP reflection methods. Of all volumetric attacks peaking at more than 100 Gbps, UDP, NTP, SSDP, and SYN floods were dominant attack methods.

In 2018, UDP flood attacks overtook SYN flood attacks to contribute the largest proportion of volumetric attacks. In 2017, SYN flood attacks dominated this realm because of prevalent use of large SYN packets. However, this type of attack has a distinct pattern and is so easy to identify and block. This change in the dominant position of attack types reflects the constant iteration and evolution of offensive and defensive techniques and methods. At the same time, the security of IoT is becoming an increasingly serious issue as many connected devices of low power consumption can be converted to bots. Also contributing is bandwidths keep expanding all around the world. All these factors make UDP floods, which leverage the connectionless UDP protocol while providing low resource consumption and high bandwidth usage, a favored type of DDoS attack.

Figure 3.10 Distribution of DDoS attack types by consumed bandwidth



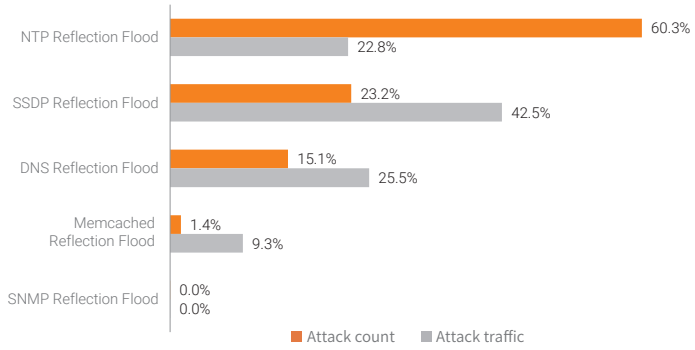
Source: NSFOCUS ATM

3.2.3 Reflection Attacks

In 2018, the number of reflection attacks experienced a sharp drop, accounting for only 3% of the total DDoS attacks, but still contributed 10% of total DDoS traffic. Due to their amplification effect, reflection attacks are still a hazard that cannot be ignored.

In terms of the attack count, NTP reflection attacks topped the list, accounting for 60% of all reflection attacks. In terms of the attack traffic, SSDP reflection attacks generated 42% of traffic.

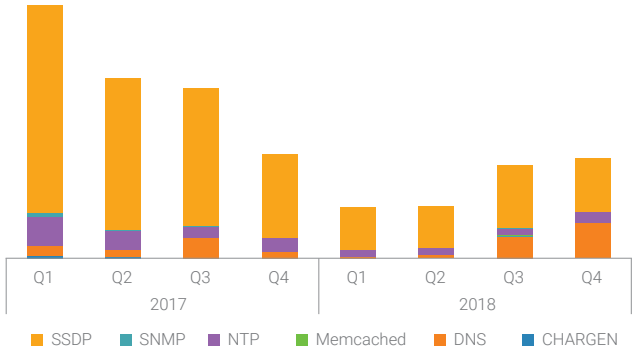
Figure 3.11 Percentages of reflection attacks by count and traffic



Source: NSFOCUS ATM

The number of active reflectors dropped 60% in 2018. Specifically, the number of SSDP reflectors decreased significantly, while that of DNS reflectors rose a bit. Within China, government crackdown on attack sources, especially SSDP reflectors, has borne fruit.

Figure 3.12 Number of active reflectors by quarter



Source: NSFOCUS ATM

As for geographic locations of reflectors used for DDoS attacks, from the global perspective, China was home to the most reflectors (46%), followed by Russia, the USA, Brazil, and Canada.

Within China, the largest percentages (18%) of reflectors were found in Shandong province, followed by Liaoning, Zhejiang, Taiwan, and Jiangsu.

Figure 3.13 Global distribution of DDoS reflectors

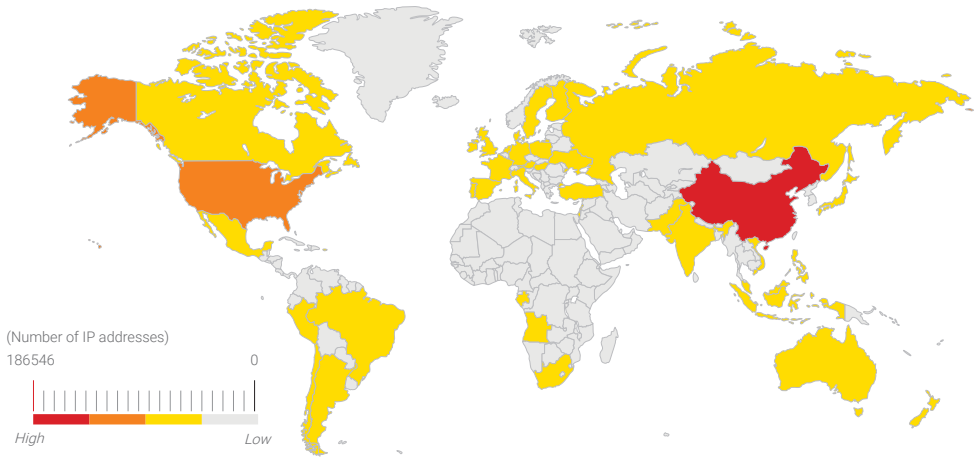
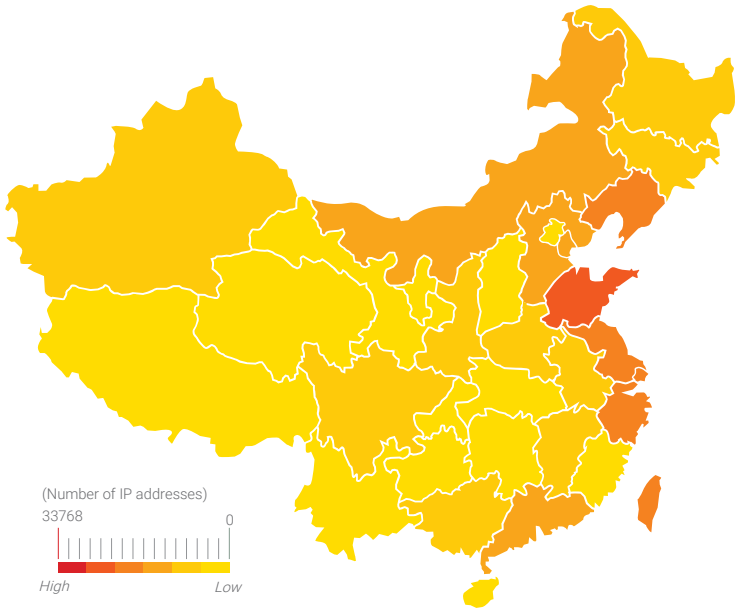


Figure 3.14 Distribution of DDoS reflectors in China



Source: NSFOCUS ATM

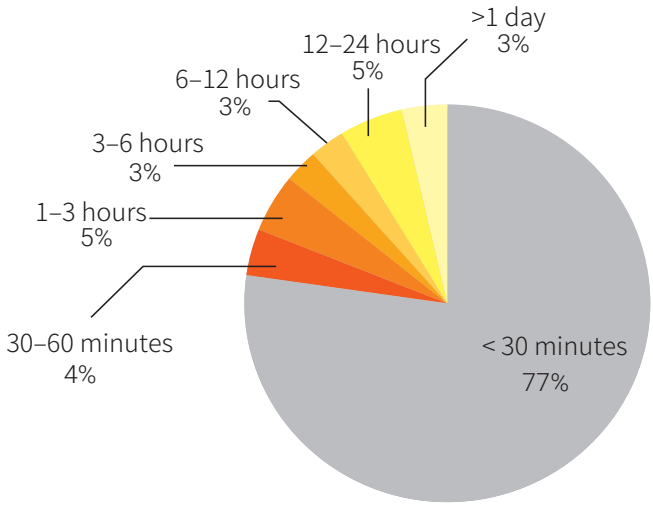
3.3 DDoS Attack Duration

3.3.1 Attack Duration Distribution

In 2018, the average duration of a DDoS attack was 42 minutes, down 17% from 2017. This indicates that DDoS attacks were upgraded in industrialization, weaponization, and efficiency and DDoS-as-a-Service gained momentum for fast growth. We noticed that the longest DDoS attack in 2018 lasted around 12 days, far shorter than attacks detected in previous years.

In 2018, short-burst attacks were on a rise. DDoS attacks shorter than 30 minutes accounted for 77% of the total number of DDoS attacks, up 33% from 2017, with the average traffic rising 1.5 times. This tells us that attackers are attaching more and more importance to cost and efficiency as they knock target services offline and cause delays & jitters with high waves of enormous volumes within short periods. In the long run, repeated burst attacks, which are more cost effective, will greatly aggravate the quality of target services.

Figure 3.15 Percentages of attacks by duration (China Telecom DamDDoS)



Source: DamDDoS

The decreasing duration of individual attacks makes it possible for attackers to accept more tasks, which characterizes Botnet-as-a-Service and DDoS-as-a-Service.[7] In the past, to create botnets, attackers actively created and spread malware to infect devices and then manipulated these devices to launch large-scale DDoS attacks as required. In this case, when to attack totally depended on the attackers' working time. A successful attack also required accumulation of botnet resources. Therefore, it is not hard to understand why improvements in antivirus software as well as new endpoint technologies led to the decline of massive laptop/workstation/server botnet-based DDoS attacks. To reverse the trend, Botnet-as-a-Service and DDoS-as-a-Service have emerged as premier rental services. In other words, they grant users without botnet resources and technical skills the ability to use a certain number of bots in a given time for a price and can deliver custom services adapted to the scale required and parameters configured by users. Thanks to the widespread use of automatic payment platforms and cryptocurrency, users can conveniently get mercenary-like attack resources by means of online payment. Such botnets not only provide the agility of launching attacks anytime and anywhere, but also make it interesting and satisfying for users to commit DDoS attacks on a whim. Imagine disgruntled employees or people in the midst of a divorce launching retaliatory attacks against the companies related to the people of their ire. All these factors contribute to a lower level of skills required for launching massive DDoS attacks and make it easier to make profits from botnets.

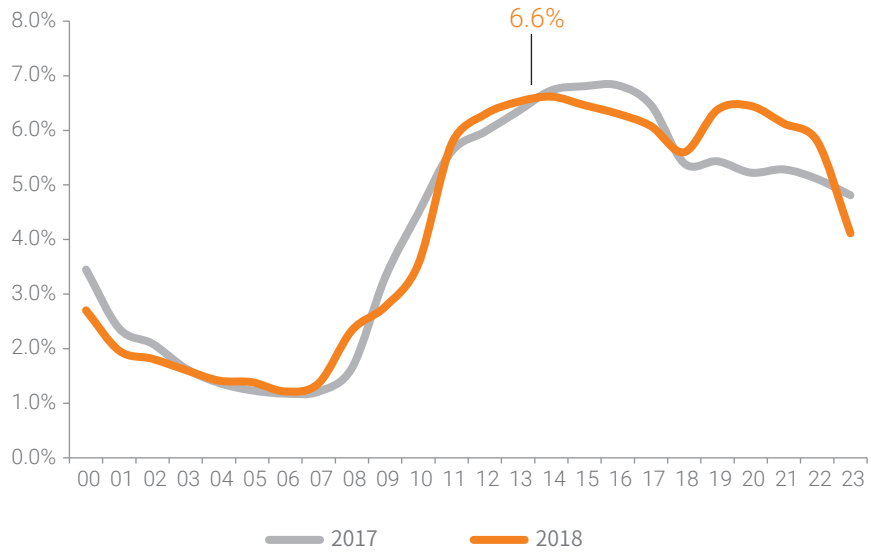
3.3.2 Attack Time Profiling

3.3.2.1 Attack Activities Within One Day

During the day from 0:00 to 24:00, the hours of 10:00–22:00 are busy for online services and the peak period of DDoS attacks, when 70% of attacks are spotted. The coincidence of busy hours of online service access with the peak period of DDoS attacks indicates that attackers time their attacks for maximum effect and impact.

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

Figure 3.16 DDoS activities in one day (China Telecom DamDDoS)

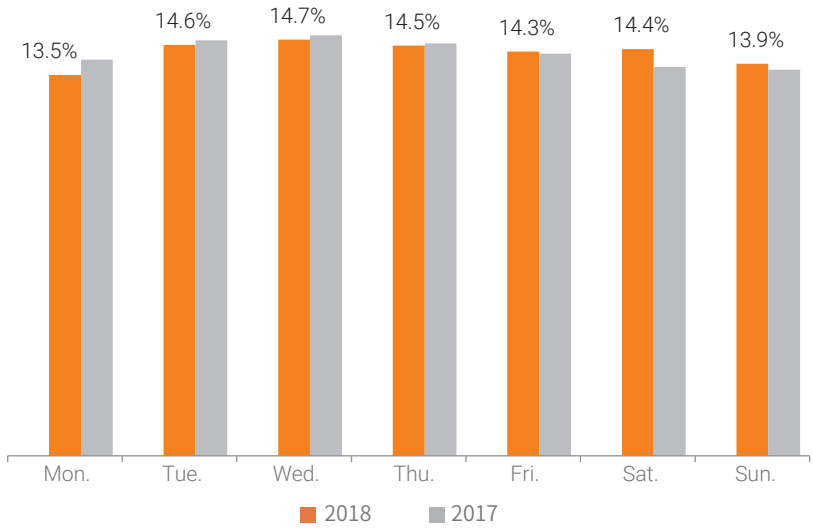


Source: DamDDoS

3.3.2.2 Attack Activities Within One Week

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

Figure 3.17 DDoS activities in a week (China Telecom DamDDoS)



Source: DamDDoS

3.4 Behavioral Analysis of Attack Sources

In the 2018 H1 Cybersecurity Insights[8], we mentioned that the number of DDoS recidivists (repeat DDoS offenders) was too large to ignore. Of all internet attack types, 25% of attackers were recidivists responsible for 40% of all attack events. As for DDoS attacks, 7% of attackers were recidivists that launched 12% of attack events. (Here, "DDoS recidivists" refer to source IP addresses that have been marked by NSFOCUS Threat Intelligence center (NTI) as DDoS attack sources.) Clearly, in DDoS attacks, the proportion of recidivists decreased in 2018, indicating a lower level of resource reuse. This can be attributed to two factors:

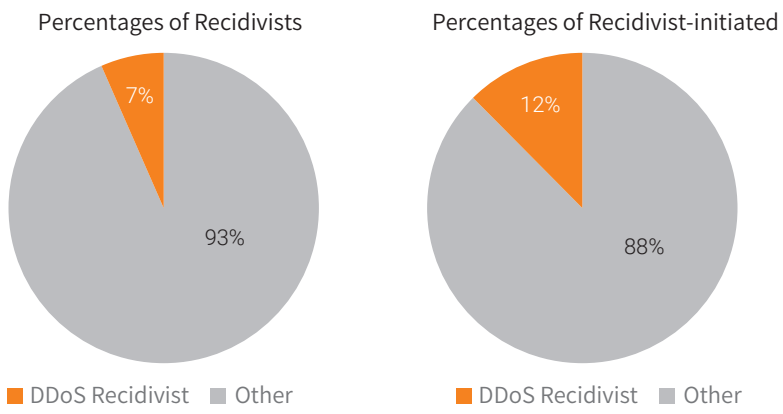
8 https://nsfocusglobal.com/2018-h1-cybersecurity-insights/

(1) There are large quantities of attack resources publicly available via the Internet, and attackers can easily obtain such resources through repeated scanning, making it unnecessary to retain attack resources for a long time. Most recidivists are long-lasting harmful resources on the Internet that are very easy to leverage for attackers around the world.

(2) DDoS attacks are typically the last step to complete the kill chain. When hosts/devices are leveraged to conduct DDoS attacks, maintenance personnel can easily spot them and promptly fix the problem. Therefore, a large proportion of bot hosts previously used in a DDoS attack will be abandoned later, making it necessary for hackers to rescan and infect hosts to expand the botnet size.

Furthermore, we notice that, regardless of the attack type, the proportion of attacks initiated by recidivists is often twice that of number of recidivists themselves. Recidivists should be considered quite threatening, and their activities should be closely monitored.

Figure 3.18 Percentages of recidivists and that of recidivist-initiated attacks

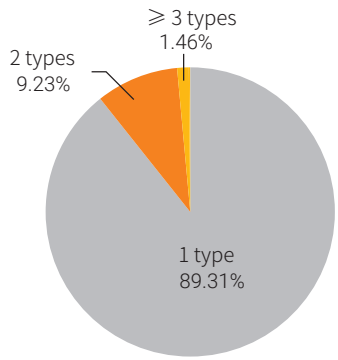


Source: NSFOCUS ATM and NTI

3.4.1 Anomalous Behavior

Attack resources used in DDoS attacks are typically involved in only one attack type. Among all DDoS sources, 89% have conducted only one type of anomalous activity and only a small proportion are found to have engaged in several (up to six) types of anomalous activity.

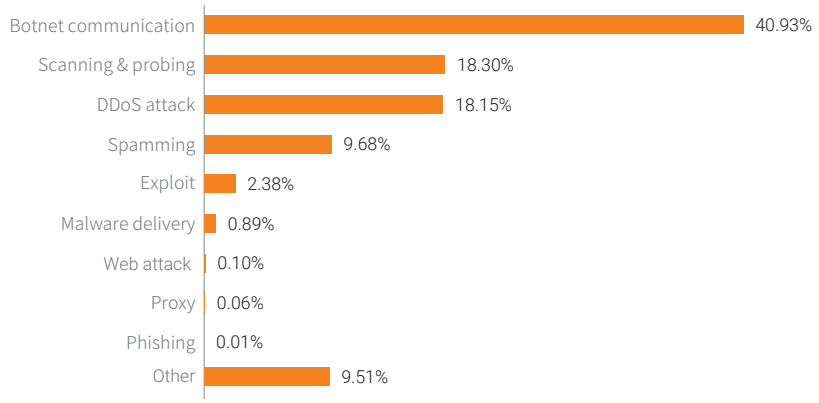
Figure 3.19 Distribution of DDoS recidivists by the number of attack types



Source: NSFOCUS ATM and NTI

As shown in Figure 3.20, 41% of attack sources were controlled botnets; 18% have conducted scanning, which is the preparation step for subsequent intrusions by collecting system information and vulnerability information of target machines; another 18% were marked by NTI as to have repeatedly conducted DDoS attacks because they contain vulnerabilities that can be remotely controlled and were left unfixed, or because they have reflection capability.

Figure 3.20 Percentages of DDoS recidivists' behavior types

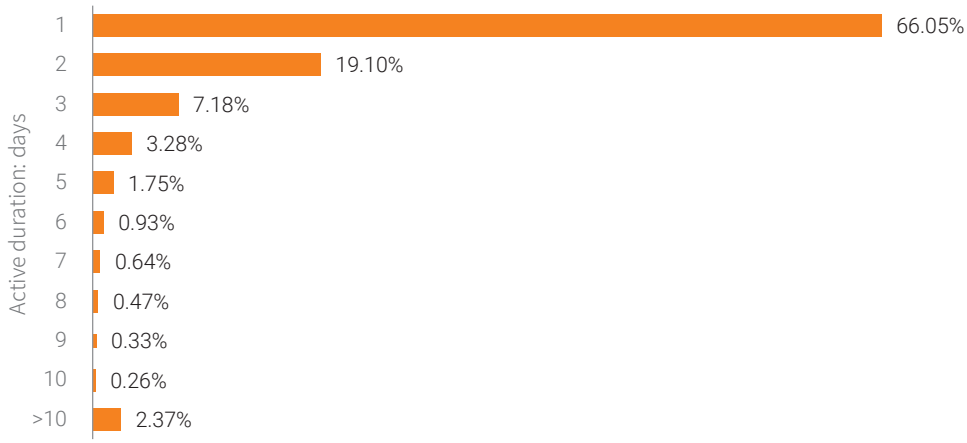


Source: NSFOCUS ATM and NTI

3.4.2 Activity

From monitoring of attack source activity, we see 10 days is a clear-cut divide for activity. Specifically, the proportion of attack sources active for less than 10 days is 98%, and that of attack sources active for more than 10 days (up to 280 days) is 2%. 95% of attack sources remain active for 1–5 days. This infers that in order to keep attack resources viable and prevent them from being blacklisted by defenders, attackers tend to use the hit-and-run strategy, specializing in multiple short attacks. Also suggested is that there are a wide range of vulnerable IP addresses on the Internet, making it easy for attackers to obtain such resources at a very low cost.

Figure 3.21 Distribution of short-duration attacks



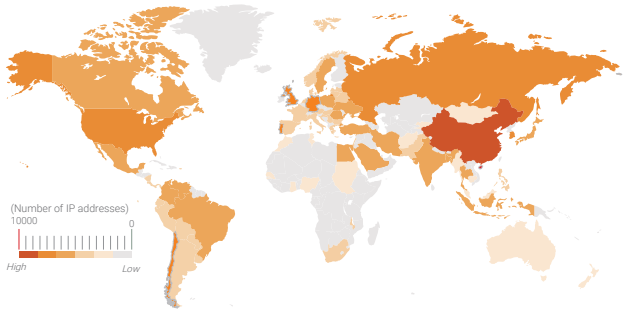
Source: NSFOCUS ATM

3.4.3 Geographic Distribution

According to distribution of activity time of attack source IP addresses, attack sources active for over 10 days are regarded as highly desirable. They often contain an obvious security risk which is easily exploited, thus posing greater threats.

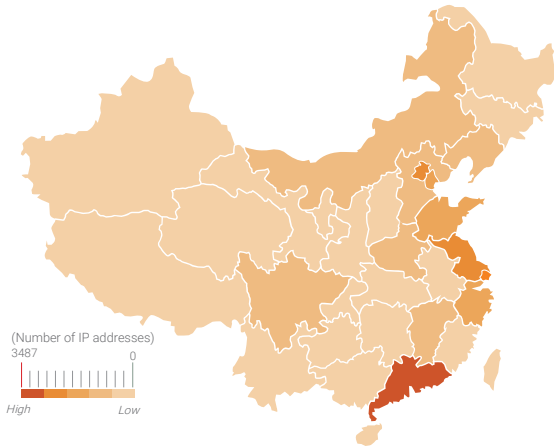
Globally, highly active attack sources are mostly distributed in China, the USA, and Russia. In China, they are mostly in coastal provinces and economically developed regions, such as Guangdong, Jiangsu, and Beijing. With a larger network infrastructure than other regions, even with similar protections, networks in these regions are more vulnerable than in other regions due to a much greater number of potentially vulnerable devices.

Figure 3.22 Global distribution of highly active attack resources



Source: NSFOCUS ATM and NTI

Figure 3.23 Distribution of highly active attack resources in China



Source: NSFOCUS ATM and NTI

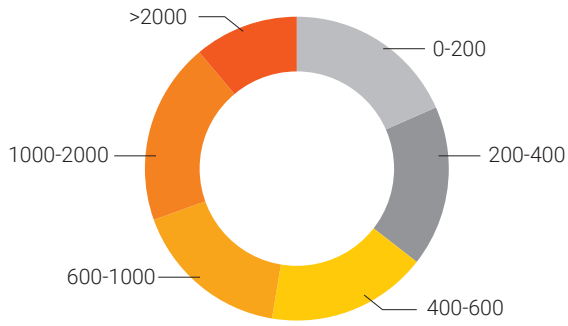
3.4.4 IP Chain-Gang Behavior

IP Chain-Gang attacks refer to the large-scale attacks launched using certain attack methods through relatively monopolized attack resources. Unlike common attack events initiated by a single attacker, IP Chain-Gangs typically pursue intelligence and economic targets. Therefore, NSFOCUS feels that research into attack gang behavior based on their attack characteristics and history will be useful in predicting future IP Chain-Gang behavior. In the report, Behavior Analysis of IP Chain-Gangs[9], recently released by NSFOCUS, we introduce the concept of modeling gang behavior based on gang size, attack traffic, attack count, and victims.

IP Chain-Gang Size

According to the overall distribution of gang sizes, most IP Chain-Gangs have less than 1000 members, except for one gang which has over 26,000 members.

Figure 3.24 Size distribution of IP Chain-Gangs

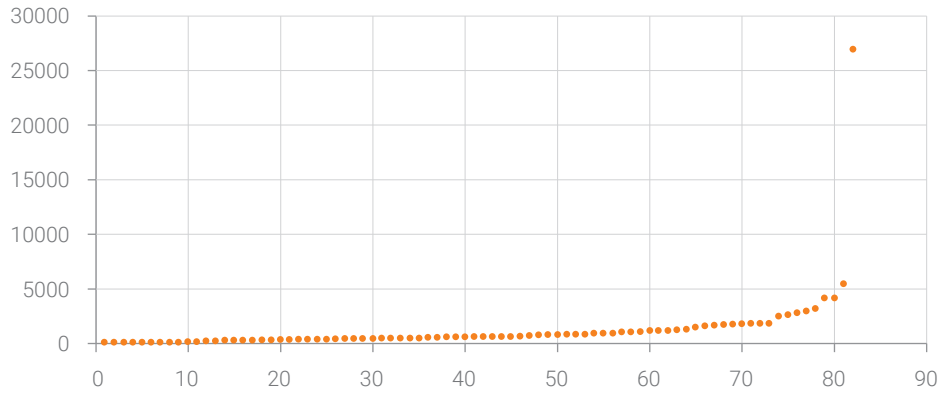


Source: NSFOCUS ATM and NTI

Figure 3.24 shows the size distribution of the IP Chain-Gangs identified by NSFOCUS. Each point represents a gang, with a total of 82 gangs found to date.

9 https://nsfocusglobal.com/behavior-analysis-ip-chain-gangs/

Figure 3.25 Size distribution of IP Chain-Gangs

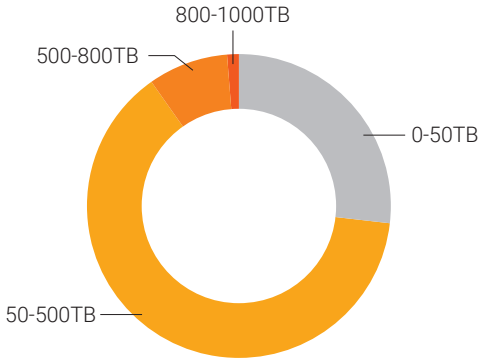


Source: NSFOCUS ATM and NTI

Total Attack Volume

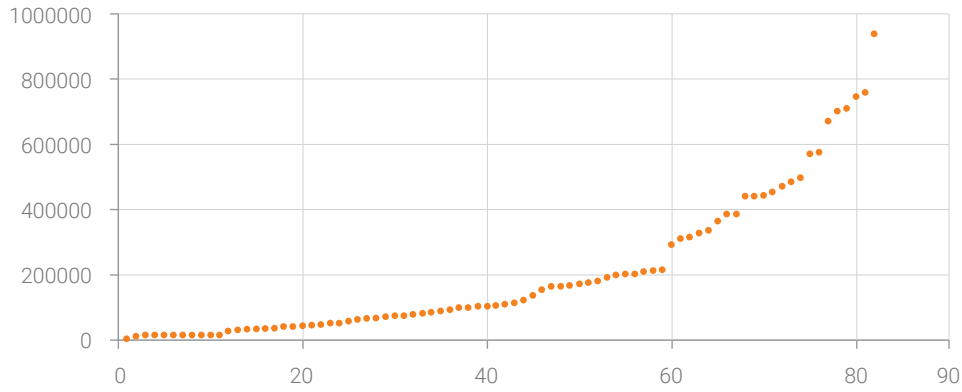
The total attack volume of each gang includes the traffic generated by all attacks launched by each member. Though the total attack volume varies, the total attack volume of most IP Chain-Gangs has exceeded 50 Tbps.

Figure 3.26 Total attack traffic distribution



Source: NSFOCUS ATM and NTI

Figure 3.27 Total attack volume distribution (Gbps)

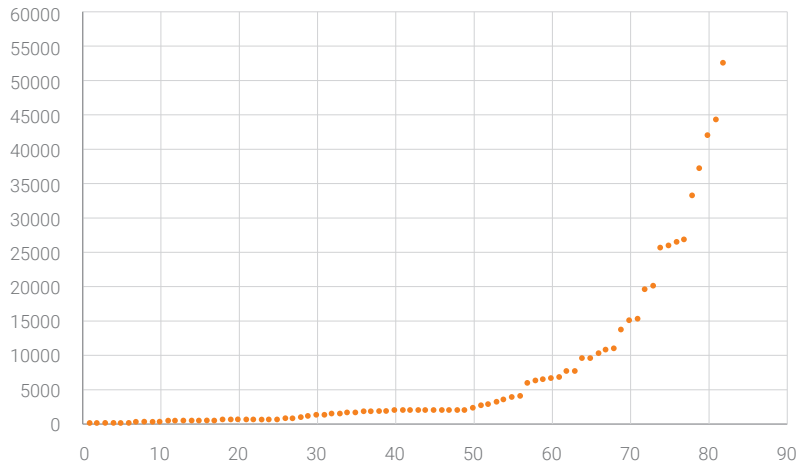


Source: NSFOCUS ATM and NTI

Attack Count

As shown in Figure 3.27, the number of attacks launched by each member of nearly 60 IP Chain-Gangs was less than 5000. It was somewhat surprising that 80% of all attacks were launched by only 20% of gangs.

Figure 3.28 Attack count distribution



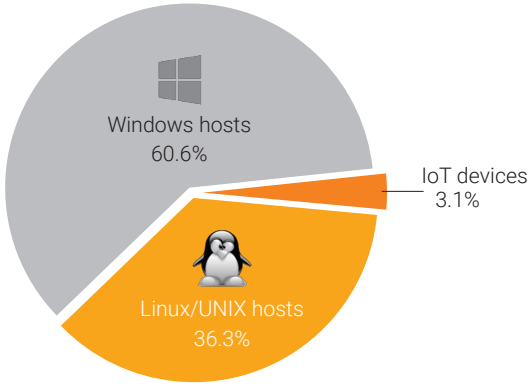
Source: NSFOCUS ATM and NTI

3.5 Analysis of IoT Attack Sources

3.5.1 Participation of IoT Devices in DDoS Attacks

According to NSFOCUS's IoT threat intelligence, some DDoS attacks are associated with IoT devices. By further analyzing the proportion of IoT devices in DDoS attack source IP addresses, we find that 3.14% are IoT devices. Although this proportion is relatively small, compared to the large base of DDoS attack source IP addresses, the threat of IoT device-based DDoS attacks cannot be overlooked.

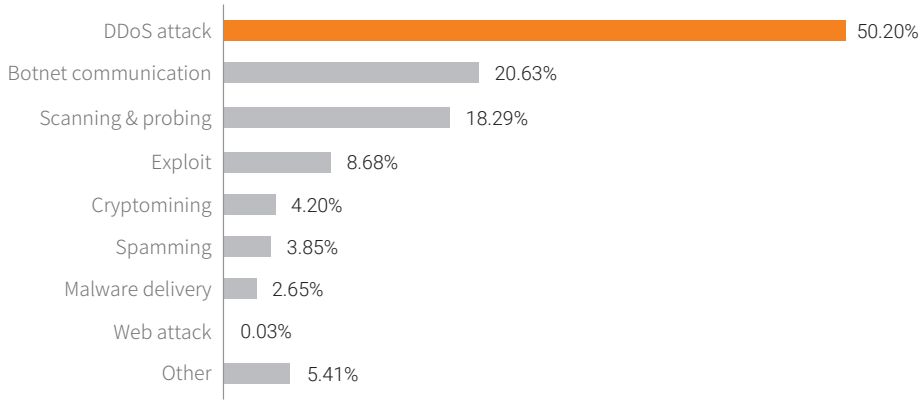
Figure 3.29 Percentages of IoT devices as source IP address of DDoS attacks



Source: NSFOCUS ATM and NTI

We detected that the total number of IP addresses of abnormal IoT devices was 408,685 worldwide, accounting for 0.94% of global IoT devices. The number of IP addresses involved in IoT device-based DDoS attacks was 205,167, reaching 50.20% of the total number of IP addresses of abnormal IoT devices. As shown in Figure 3.29, among different types of IoT device-based attacks, DDoS attacks take up the largest proportion. It is thought that abnormal IoT devices are mainly exploited to launch DDoS attacks.

Figure 3.30 Percentages[10] of abnormal IoT device-based behaviors



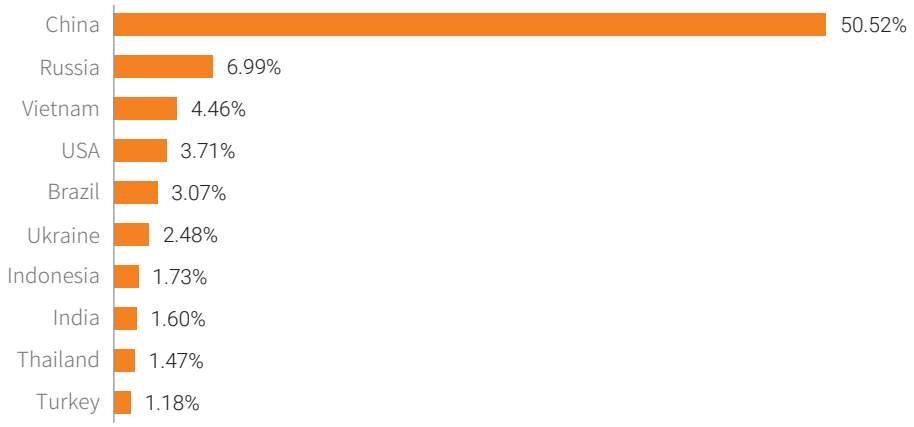
Source: NSFOCUS ATM and NTI

3.5.2 Geographic Distribution of IoT Devices Involved in DDoS Attacks

By analyzing the global distribution of IoT devices involved in DDoS attacks, we find that most of these devices are in China, with over 90,000 IP addresses identified. China, Russia, Vietnam, the USA, and Brazil are the top 5 countries housing the most IoT devices. It should be noted that NSFOCUS is aware that an IoT device may change IP addresses over time and are researching mechanisms to better fingerprint IoT devices in the future.

10 Since some devices have several abnormal behaviors, the accumulative percentage in this figure exceeds 100%.

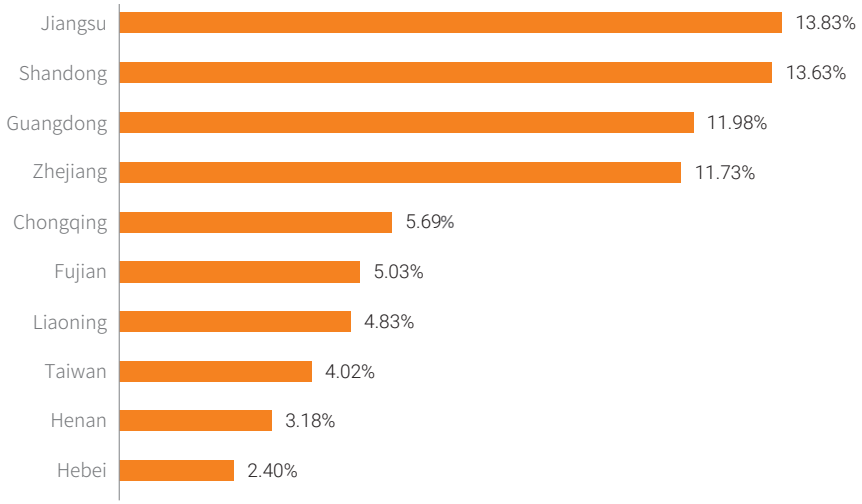
Figure 3.31 Global distribution of IoT devices involved in DDoS attacks



Source: NSFOCUS ATM and NTI

As shown in Figure 3.31, China had the most IP addresses belonging to IoT devices involved in DDoS attacks. If we narrow down the scope to China alone, Jiangsu, Shandong, Guangdong, and Zhejiang were top 4 provinces with the most IoT IP addresses.

Figure 3.32 Distribution of IoT devices involved in DDoS attacks in China



Source: NSFOCUS ATM and NTI

In 2018, Guangdong, Jiangsu, Shandong, and Zhejiang boasted the most provincial Gross Domestic Product (GDP in China). According to NSFOCUS's 2018 Annual IoT Cybersecurity Report, this has a lot to do with the popularity of IoT devices and the prosperity related to high technologies and services. In particular, economically developed provinces have the financial resources and motivation to procure and deploy IoT devices and related intelligent systems. The output value of the tertiary industry is an important part of their provincial GDP in Guangdong, Jiangsu, Shandong, and Zhejiang. Therefore, it makes sense that IoT device deployment tracks with their level of economic growth.

Thus, with the robust economic development in these provinces, the popularity of IoT devices improves accordingly, hence the increased number of IoT devices deployed in these provinces. As shown in Figure 3.30, DDoS attacks are the most frequent abnormal behavior for IoT security. Therefore, the more a region is economically developed and the more IoT devices it has, the more IoT device-based DDoS attacks it will both generate and suffer.

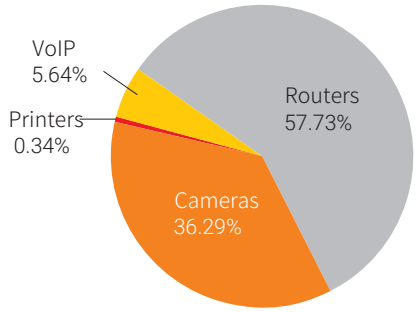
3.5.3 Distribution of IoT Device Types Involved in DDoS Attacks

Routers and cameras are the major targets of IoT device-based attacks. In 2018, many botnets exploited numerous medium & high router and camera vulnerabilities to penetrate these devices. For example, in February 2018, by exploiting CVE-2017-17215 and CVE-2014-8361 vulnerabilities, JenX[11] infected Huawei HG532 routers and devices running Realtek SDK to form botnets. It was reported that at least 29,000 devices were controlled by JenX. The new botnet IoTroop[12] emerging at the end of 2017 exploited partial Mirai code. Like Mirai, IoTroop targets network devices such as routers and cameras from TP-Link, Avtech, MikroTik, Linksys, Synology, and GoAhead. According to Insikt Group[13], this botnet consists of infected MikroTik routers (80%) and other types of IoT devices (20%), including routers from Ubiquity, Cisco, and ZyXEL.

11 https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/jenx
12 https://research.checkpoint.com/iotroop-botnet-full-investigation/
13 https://www.hackeye.net/threatintelligence/13150.aspx

Regarding device types, the total number of IoT devices involved in DDoS attacks was more than 230,000. As we said, the predominant types were routers and cameras, accounting for more than 94%. This is consistent with the type distribution of IoT devices.

Figure 3.33 Distribution of IoT devices involved in DDoS attacks by type



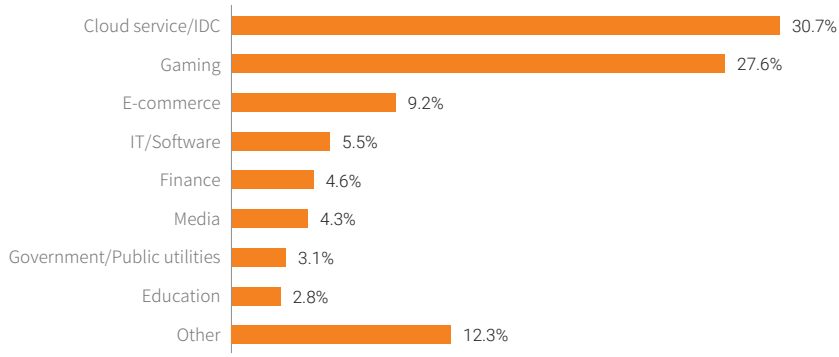
Source: NSFOCUS ATM and NTI

3.6 Industrial Distribution of Attack Targets

From an industry perspective, cloud service/Internet data center (IDC), gaming, and e-commerce are top 3 industries suffering the most DDoS attacks.

Gaming and e-commerce industries are most favored by attackers for DDoS attacks because they have high requirements for prompt data processing and business continuity, must face fierce competitions with peers, boast volumetric traffic every day, and have good financial liquidity. Generally, hired by a vicious competitor, attackers make profits by launching attacks against other competitors. The competitor aims to seize resources by degrading the quality of service of their counterparts. These are also top criteria for identifying ransom targets.

Figure 3.34 Attack distribution by industry



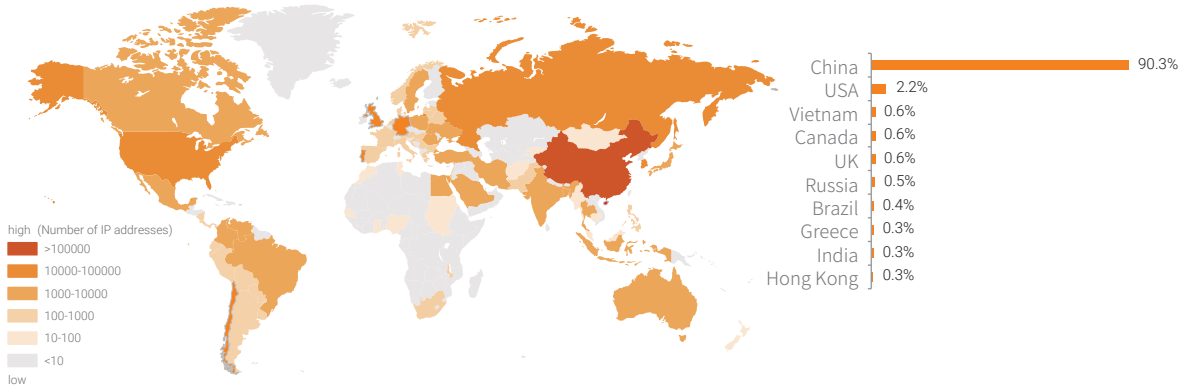
Source: NSFOCUS ATM and NTI

3.7 Geographic Distribution of DDoS Attacks

3.7.1 Controlled DDoS Attack Sources

Controlled DDoS attack sources are not necessarily members of botnets but are definitely under some type of malicious remote control. China still hosted the most controlled DDoS attack sources (90%) in 2018, followed by the USA and Vietnam.

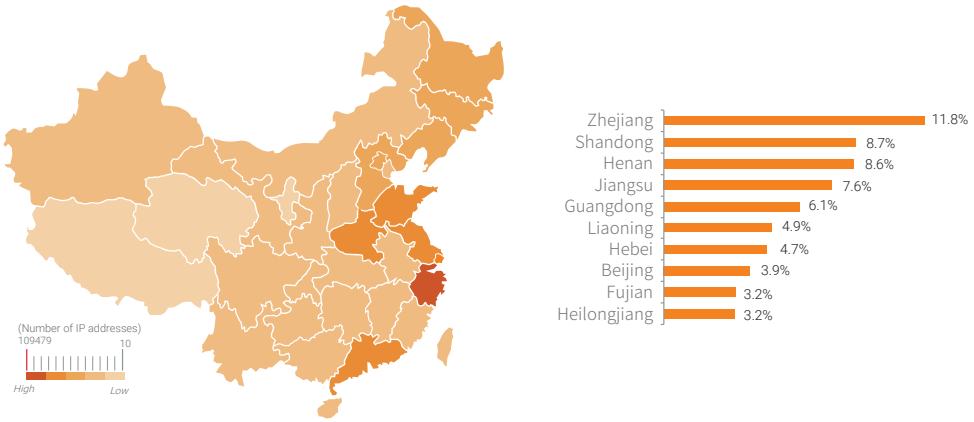
Figure 3.35 Global distribution of attack source IP addresses



Source: NSFOCUS ATM

In 2018, Zhejiang, Shandong, and Henan were top 3 Chinese provinces hosting the most controlled attack sources.

Figure 3.36 Distribution of attack source IP addresses in China

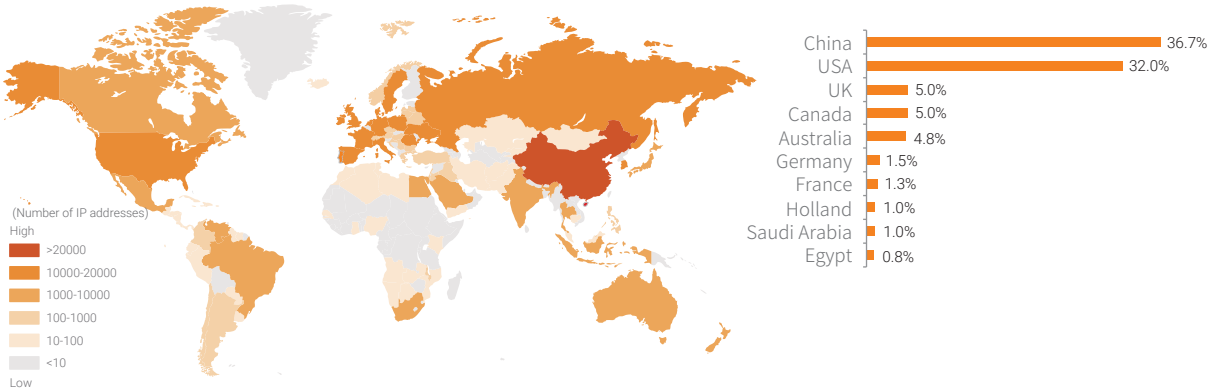


Source: NSFOCUS ATM

3.7.2 DDoS Attack Targets

In 2018, China was the most severely attacked country, seeing 36% of total worldwide attacks, followed by the USA (32%).

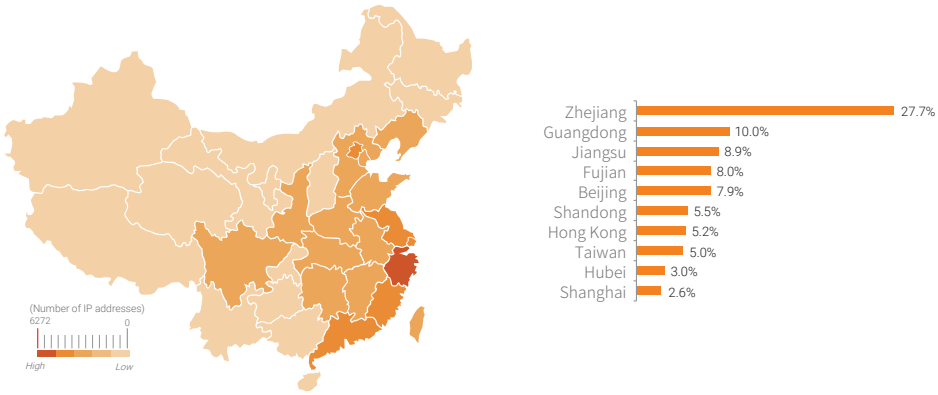
Figure 3.37 Global distribution of attacked IP addresses



Source: NSFOCUS ATM

In China, Zhejiang was the most severely attacked province, followed by Guangdong, Jiangsu, Fujian, and Beijing. China's eastern coastal areas have always been the most favored targets of DDoS attacks, again likely due to their economic prosperity.

Figure 3.38 Distribution of attacked IP addresses in China

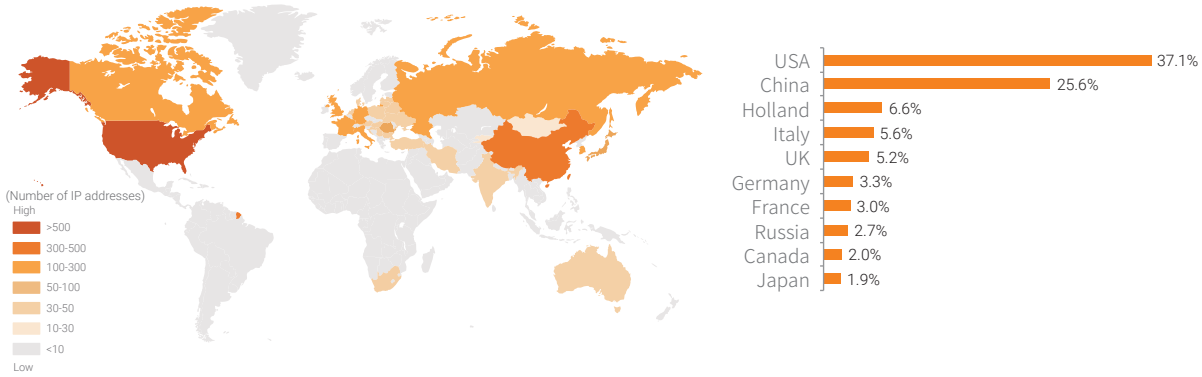


Source: NSFOCUS ATM

3.7.3 DDoS Command & Control Servers

Globally, the USA, China, and Holland were top 3 countries with the most IP addresses of the DDoS command & control (C&C) servers, making up 70% of the world's total.

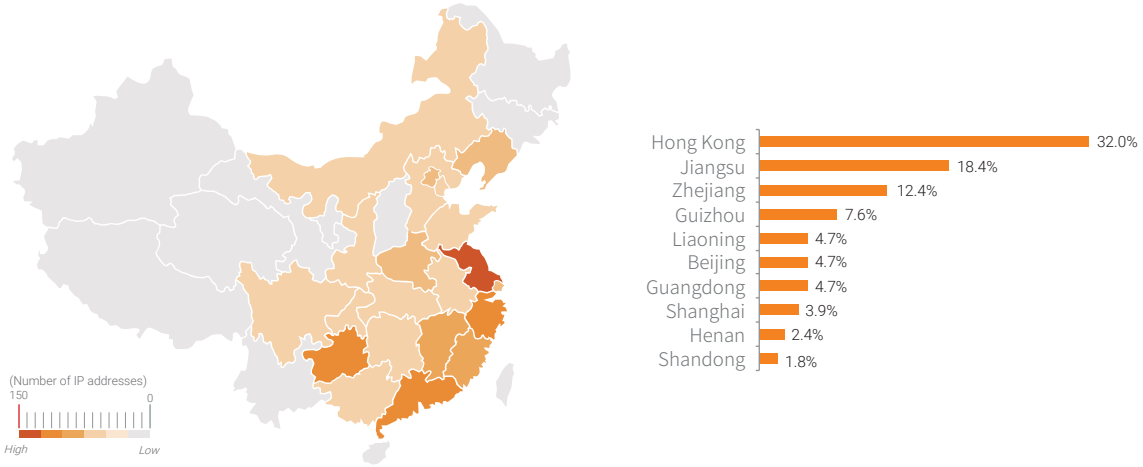
Figure 3.39 Global distribution of DDoS C&C servers



Source: NSFOCUS ATM

In China, Hong Kong, Jiangsu, and Zhejiang ranked top 3, occupying over 60% of traceable DDoS C&C servers in China.

Figure 3.40 Distribution of DDoS C&C servers in China



Source: NSFOCUS ATM

4

DDoS Attack Protection and Mitigation

Behind DDoS attacks, there are complex economic interests in the underground industry. Therefore, effective governance needs to start from multiple dimensions, including policy, industry, resource, and technical dimensions. This chapter dwells upon how to mitigate DDoS attacks from the following perspectives.

4.1 Upgrading the Network Architecture and Technology

During the development of computer technology and the Internet, inherent and developed vulnerabilities in the architecture and technology provided the hotbed of DDoS attacks.

For example, the lack of effective methods of IP address identification and traceability has resulted in the widespread use of various attack methods with address spoofing as the core. In the existing network architecture, spoofed IP addresses can hide the identity of attackers. Reflection attacks are launched via requests from spoofed IP addresses.

In addition, the lack of unified network traffic control led to the delay of DDoS attack detection, alert, and response, hence the broadened attack impact. Today large-scale and distributed DDoS attacks make it difficult for existing heterogeneous and complex network architectures to detect their early signs in time. When a DDoS attack is launched across the board, it is difficult to quickly isolate malicious traffic and target devices.

Fortunately, with the development of DDoS mitigation technology, computing technology and the establishment of related standards, the preceding problems have been greatly mitigated. For example, the solution of separating the network data plane from the management plane represented by software-defined networking (SDN) technology lays a critical foundation for the global and intelligent management of network traffic and network nodes; the core capabilities of cloud computing (such as resource virtualization) provide support for the isolation, fault tolerance, and restoration of cloud-based network resources. The emergence of various algorithms and standards for packet labelling and filtering helps effectively reduce the transmission paths of packets with a spoofed IP address.

4.2 Exposing Service Management

Launching DDoS attacks requires large-scale attack resources, and the various open services in the Internet are potential resources available to attackers. For example, reflective DDoS attacks are usually launched by exploiting open public services on the Internet or accidentally exposed intranet services. The number of potentially exploitable service resources exposed to the Internet is enormous. For open services, such as DNS and NTP services, it is necessary for relevant departments and asset owners to investigate the service vulnerability, strengthen the control of response policies, and deploy effective detection mechanisms, so as to prevent malicious use. For accidentally exposed intranet services and protocols, such as SSDP, Memcached, and intranet DNS, relevant enterprises should enhance network isolation measures and improve their personnel's security awareness, in a bid to prevent accidental exposure of intranet services.

4.3 Dismantling Botnets

Botnets are always the main force for launching DDoS attacks in the underground industry. By releasing various worms, viruses, and malware, attackers can infect and control a large number of zombies. To dismantle botnets, two mitigation strategies need to be implemented:

(1) we need to start with malicious samples, analyze attack methods, and strengthen protection measures at each stage of the kill chain;

(2) we need to improve proactive protection policies, monitor botnet trends, and provide early detection, alerting, and trackback of DDoS attacks.

For example, through honeypot and honeynet technology, we can proactively obtain malicious samples and capture malicious traffic behaviors. Taking advantage of correlative analysis, we can identify the attacker's purpose, crack his/her attack methods, and break the kill chain.

4.4 Analyzing Traffic

Analysis capability is of great importance to DDoS attack protection and governance.

With the increasing demand of networks and the rapid development of IPv6 and 5G technologies, network bandwidth is growing rapidly. In this context, traditional traffic analysis technology & methodology can no longer keep up with networks with huge amounts of incoming and outgoing traffic. For example, deep packet inspection (DPI) technology incurs high CAPEX costs, and the analysis capability of traditional deep flow inspection (DFI) technology is far from adequate. This brings a great challenge to the return on investment (ROI) of traffic analysis.

For today's network traffic, tracking hotspot traffic (whether malicious or not), malware type, traffic direction, geolocation, country information, company name, device type, application name, and CDN identification are all vital data for traffic analysis. Only by acquiring, processing and understanding all the above data can managers rapidly detect and handle abnormal events. In other words, traffic analysis is an important index for measuring an organization's ability to protect against and cope with current and future DDoS attacks.

5

Summary

Summary

Profits continue to be the main motivation of attackers, who always use DDoS as a handy weapon.

Since DDoS attacks are easy to launch and can bring quick returns, they will always be favored by attackers. Industrial and technological changes indicate that DDoS attacks will take more forms on the battlefield between the offensive and defensive sides.

Therefore, DDoS protection cannot continue with the use of conventional mitigation strategies. Instead, we should

- make greater use of big data and artificial intelligence (AI) technology,
- better remediation of medium and high severity vulnerabilities especially in IoT devices,
- implement more effective early warning and detection solutions,
- take advantage of cloud cleaning services & threat intelligence,
- regularly share threat information with regulatory bodies and security vendors, thereby achieving a more coordinated defense which is a win-win scenario for all.

Only by learning to change and adapt DDoS strategies and defenses over time will organizations be able to survive the next generation of DDoS attacks. Sticking with conventional defensive strategies and not understanding the rapid changes in attacker groups and their attack techniques & patterns could result in the end of an organization. Remember, 60% of all small and medium companies that suffer a successful cyber-attack are out of business in 6 months.[14]

14 https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

Authors

DamDDoS

NSFOCUS Security Labs

Graphic Designer

NSFOCUS YanJun

中国电信·云堤 CHINA TELECOM NSFOCUS

2018 DDoS Attack Landscape