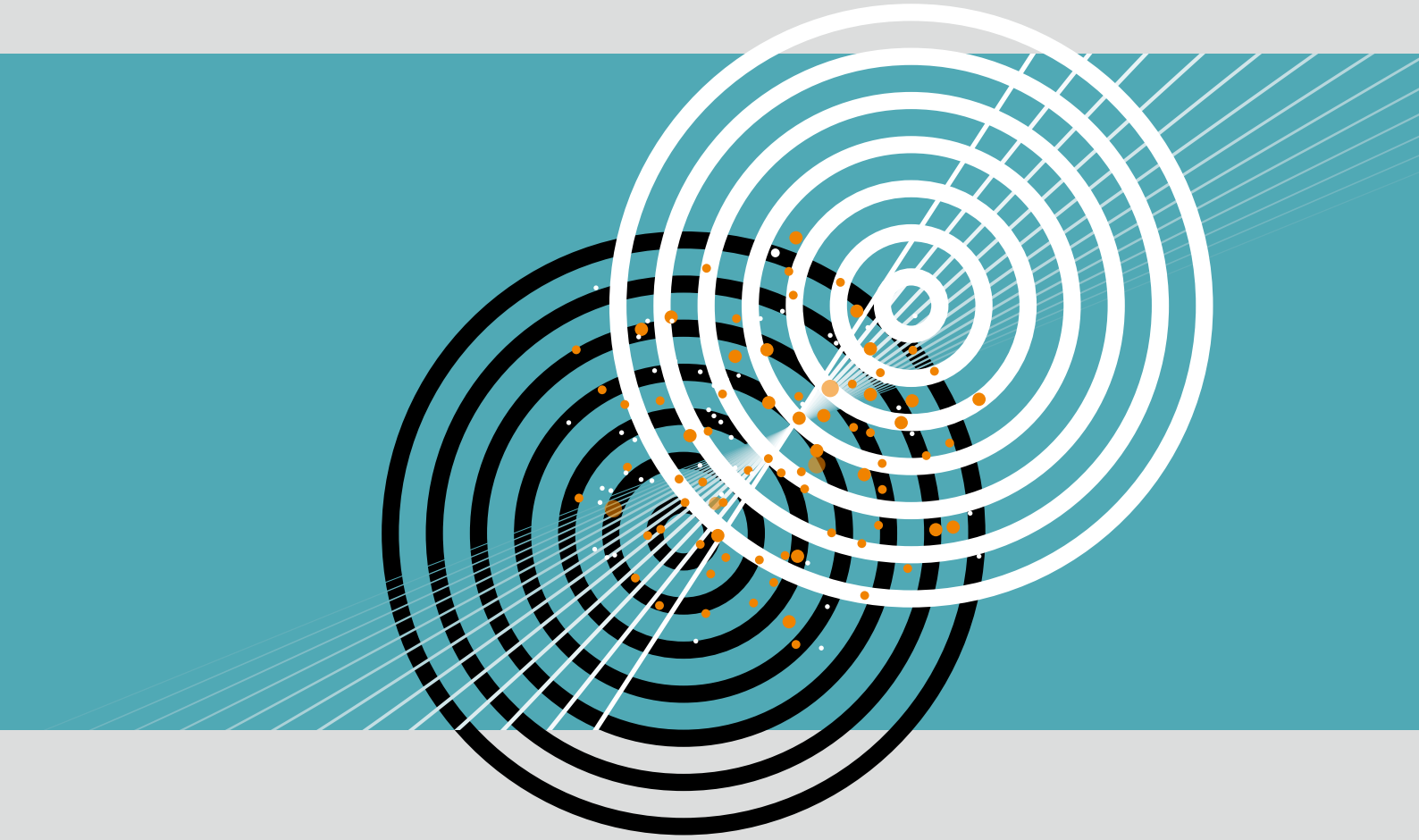


中国电信·云堤 CHINA TELECOM NSFOCUS

2017 DDoS and Web Application Attack Landscape

About YunDi of China Telecom

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 "YunDi" as a unified brand for external services.

In the past few years, China Telecom YunDi 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

Founded in April 2000, NSFOCUS Information Technology Co., Ltd. (NSFOCUS) is headquartered in Beijing. With more than 40 branches and subsidiaries at home and abroad, the company provides most competitive security products and solutions for governments, carriers, and financial, energy, Internet, education, and medical sectors, ensuring customers' business continuity.

Based on years of research in security protection, NSFOCUS has set foot in intrusion detection and prevention, security assessment, security platform, remote security O&M service, and security SaaS service areas. The company provides the intrusion detection/prevention system, anti-DDoS system, remote security assessment system, and web security protection products as well as professional security operations services for customers.

NSFOCUS Information Technology Co., Ltd. started trading its shares at China's Nasdaq-style market, ChiNext, in Shenzhen on January 29, 2014, with the name of NSFOCUS and code of 300369.

Disclaimer

To protect partners' or customers'sensitive information, all involved data has been anonymized before being analized in this paper, preventing unexpected data exposure. No partner- or customer-specific information will be seen in this paper.

Executive Summary

This report consists of eight chapters. Chapters 2, 3, and 4 present overviews on DDoS attack trends, IoT botnet development trends, and web application attack trends respectively to help readers better grasp the gist of this report. Chapters 5 analyzes trends of DDoS attacks in 2017 by detailing changes in the attack traffic, frequency, and scale from different dimensions, including the attack source, attack type, attack duration, and geographic distribution of attacks. Considering the significant impact of IoT botnets, we use a separate chapter (chapter 6) to discuss the six trends of IoT botnets in 2017 and provide a comparative analysis of IoT botnet families that made headlines in 2017 from perspectives of the hosting platform, propagation method, and potential threats. Chapter 7 revolves around the situation of web application attacks in 2017 by analyzing the attacked websites and sectors as well as the type, source, duration, and geographic distribution of such attacks. In the last chapter, we describe protection solutions developed by NSFOCUS based on its years of experience in security defenses and continuous innovations as a response to the current situation of DDoS attacks and web application attacks.

DDoS attacks and Web application attacks are the two most prominent security threats facing the Internet today.

中国电信·云堤 CHINA TELECOM NSFOCUS

2017 DDoS and Web Application Attack Landscape

DDoS
Attack Characteristics

Increase

- 640,000 TBytes of attack traffic in total, 79.4% increase over 2016
- 14.1 Gbps of average peak traffic of individual attacks, 39.1% increase over 2016
- 1.4 Tbps of maximum peak traffic among individual attacks, nearly 100% over 2016

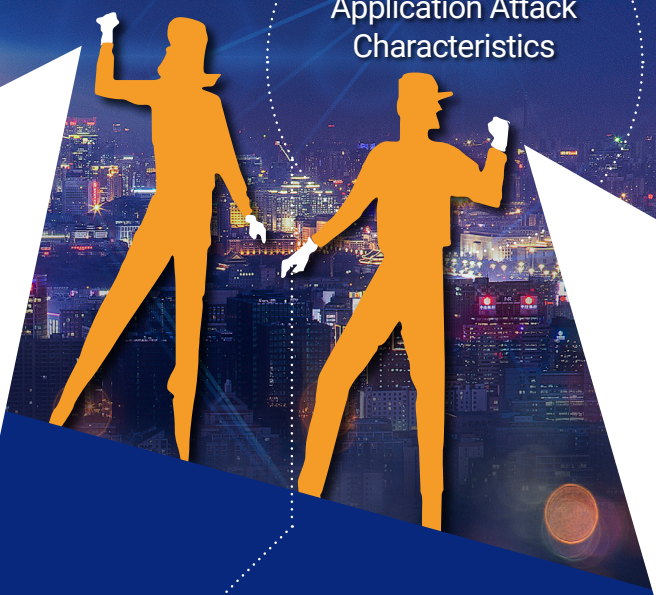
Leading

- SYN flood attack accounting for 61.6% of all attack traffic volume
- DDoS attacks ending within 30 minutes accounting for nearly half of all attacks
- Linux/Unix-like hosts or servers becoming stable attack sources (55%)
- More IoT devices involved in small attacks (29.8%)
- Home routers accounting for 69.7% of IoT attack sources

Decrease

- 207,000 attacks in total, 5.8% decrease from 2016
- 27.2% decrease of total attack traffic volume from the first to second half of 2017
- Average peak attack traffic decreasing from 16.9 to 11.2 Gbps in the first half of 2017

Web
Application Attack Characteristics



- Nearly 3/4 websites suffered at least one web application attack.
- 92.2% of web application attacks targeted Internet companies.
- Most commonly seen attacks were XSS attacks (37.7%) and injected attacks (20.7%).
- 56% of attacks exploiting server vulnerabilities lead to the disclosure of critical information.
- Apache Struts2 vulnerabilities were most frequently exploited in known framework or application exploits.

- Traditional reflection attacks dropped down, and new Memcached reflection attacks with Tbps-level traffic are rampant.
- Botnets based on IoT devices are continuously upgraded, and the threats cannot be underestimated.

1. Introduction

New Internet-based technologies and models, such as cloud computing, big data, Internet of Things (IoT), and mobile computing, are profoundly influencing transformations in the cyberspace. In this context, cyber threats keep evolving and upgrading.

Distributed denial-of-service (DDoS) attacks and web application attacks are the main security threats facing the Internet at present.

While each is distinctive in attack means and motives, the two types of attacks are closely related to rather than independent of each other. Simply put, DDoS attacks and web application attacks take place at different stages of the kill chain, with botnets as the bridge in between. Individual web application attacks, such as scanning of and injection and vulnerability exploitation for penetration into a website, may be launched for gaining access to the website for the ultimate purpose of obtaining confidential data or as a springboard to other important infrastructures of the enterprise network. The reality is that many attackers do not stop there. They often, after gaining access to the server, plant botnet malware to set up their own botnet army. As a tool for hackers to make easy money, botnets are often used for such campaigns as DDoS attacks, crypto-mining, scanning, click fraud, and spamming. Scanning servers or web applications for vulnerabilities is the first step to infection and control of hosts. More often than not, attackers use an infected device to scan the network, in a bid to find more targets.

DDoS attacks and crypto-mining, which bring direct profits to attackers, are usually found at the last stage of the kill chain. The WebLogic XMLDecoder deserialization vulnerability (CVE-2017-10271), soon after being discovered in October 2017, was exploited by hackers to spread botnet programs among WebLogic hosts for the ultimate end of crypto-mining[1]. Another example is IoT_reaper[2], an IoT botnet variant that was found active in 2017. It set up a botnet by exploiting various IoT-related vulnerabilities, including the GoAhead web server vulnerabilities (CVE-2017-8221 through CVE-2017-8225)[3] contained in certain web cameras. Note that one of the most important functions of IoT_reaper is to launch DDoS attacks.

In this report, we present the status and trends of both DDoS attacks and web application attacks, in hopes of informing cybersecurity professionals' security operations and organizations' efforts in continuously improving their own cybersecurity techniques and systems.

1 http://toutiao.secjia.com/weblogic-host-mining
2 https://research.checkpoint.com/new-iot-botnet-storm-coming/
3 https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

DDoS attacks increase in size in 2017, attack traffic peaks a new record high, and enterprises face greater DDoS threats.

2. Overview of DDoS Attacks in 2017

1. 2017 vs. 2016

- The total number of attacks reached 207,000, down 5.8%.
- The total volume of attack traffic reached 640,000 TB, up 79.4%.
- The average peak traffic of individual attacks increased 39.1% from 10.1 Gbps to 14.1 Gbps.
- The maximum peak traffic in a single attack nearly doubled from 738 Gbps to 1.4 Tbps.
- The average attack duration increased 36% from 8.8 hours to 12 hours.
- The longest attack lasted 386 hours, less than 50% of the previous year's record (880 hours).
- SYN flood traffic increased significantly, accounting for 88.7% of the total traffic generated by super large attacks (peak traffic ≥ 300 Gbps) in 2017, twice of the percentage in 2016.

2. 2017 H2 vs. 2017 H1

- The total volume of attack traffic decreased 27.2%.
- The average peak traffic decreased 33.7% from 16.9 Gbps to 11.2 Gbps.
- The maximum peak traffic decreased from 1.4 Tbps to 713 Gbps.
- The average attack duration increased from 8.8 hours to 15.6 hours.

3. Key Findings

Finding 1: In 2017, the DDoS attack size steadily grew and the peak traffic repeatedly hit new record highs.

On the one hand, DDoS attacks begin to be industrialized and DDoS as a service is becoming a trend. On the other hand, the ever expanding IoT provides an increasing number of sources that can be exploited to launch attacks. At the same time, hackers keep upgrading IoT botnets. All these reduce the attack cost and make it possible to constantly expand the attack size. This trend indicates that DDoS attack threats facing enterprises will grow with the time.

Finding 2: DDoS attackers were obviously profit-driven and sensitive to regulatory policies.

The first half of 2017 was infested with DDoS attacks, which, however, somewhat abated in the second half. Compared with 2017 H1, the latter six months saw a total volume of attack traffic decrease by 27.2% and the average peak traffic of individual attacks by 33.7%. Take medium-scale attacks as an example. The number of sources in the fourth quarter decreased by 75.8% from the second quarter. In 2017 H2, the number of Windows and Linux/UNIX hosts as attack sources significantly dropped, but that of IoT devices as attack sources of small attacks soared despite that the former excel in computing performance. Deterred by state policies and strict regulatory measures, hackers on the black market switch their high-performance botnet resources from DDoS attacks that have a high crime cost to crypto-mining that is less costly and risky but more profitable. This shows that hackers are sensitive to regulatory policies and motivated by financial gains when allocating attack resources.

Finding 3: Linux/UNIX hosts and servers constituted a strong base (55%) of DDoS attack sources. IoT devices were more frequently seen in small attacks (29.8% in small attacks and 10.3% in large attacks). Windows servers were often present in large attacks.

Finding 4: Among all IoT devices as DDoS attack sources, home routers or modems took up the largest proportion (69.7%). While the IoT is usually involved in small DDoS attacks, we can never let our guards down on the threat posed by IoT botnets due to the severity of IoT-related security issues (large quantities of vulnerabilities that are difficult to fix), diversity and magnitude of IoT devices, and constant upgrade of IoT-targeting malware.

Finding 5: Most DDoS attacks took place in busy hours of a day to maximum the attack effect. Specifically, attacks were often launched during business hours and leisure hours (10:00–22:00) (75.7%) on weekdays.

Finding 6: The trend of traditional reflection attacks, such as those based on the Network Time Protocol (NTP), slowed down, while modern ones that abused Memcached servers surged and related peak traffic hit a new record high of 1.35 Tbps.

Finding 7: China housed the most controlled attack sources, which accounted for about 50% of the global total. Shandong and Xinjiang first made it into top 5 in China.

Finding 8: China was most targeted, receiving 60% of DDoS attacks. Within China, Zhejiang saw the largest proportion of DDoS attacks and Fujian first made it into top 3.

3. Overview of IoT Botnet Trends in 2017

There will be more and more threats from IoT botnets. From the attack source data, IoT devices are obviously more frequently used in small DDoS attacks. But we cannot let our guards down for this reason. According to NSFOCUS's 2017 IoT Security Report, a total of about 62 million IoT devices were exposed on the Internet in 2017, most of which were routers (49 million), including 10.92 million from China. Assume that only 1% of these devices are infected by malware in China. Then attackers can easily launch DDoS attacks peaking at Tbps level by leveraging these infected devices. In fact, the current security status of IoT devices is rather worrying and related security issues are seldom fixed in time. This provides a far higher chance of infection than the assumed 1% for these devices. These resources, once controlled by cyber criminals, will pose inestimable dangers. To add fuel to the fire, new IoT botnet variants keep emerging with increasingly high capabilities.

We predict that IoT botnets will evolve in the following trends:

- Upgraded way of infection: from weak password cracking to 0-day vulnerability exploitation
- Further expansion of the infection platform: able to be spread across platforms
- Being more covert: use of more covert scanning techniques and sandbox techniques
- Constant upgrade of arsenals: integration of reflection attack capabilities
- Black market more energetic in scrambling for Iot Botnet resources
- More extensive threats from the IoT due to the gigantic size and outstanding security issues (lots of vulnerabilities that are difficult to fix) that make it easy to infect and control IoT devices

In 2017, 73.6% of websites suffered web application attacks, and 92.2% of such attacks targeted the Internet industry.

4. Overview of Web Application Attacks in 2017

1. 73.6% of websites suffered web application attacks.
2. 65.9% of websites were attacked because of known web vulnerabilities in web servers or web frameworks.
3. 92.2% of web attacks targeted Internet enterprises. This, however, does not mean other sectors are safe from web attacks, which are usually the first step to compromising enterprise intranets.
4. Cross-site scripting (XSS) attacks accounted for 37.7%. Although XSS has been downgraded from A3 to A7 in terms of risks, it is still most frequently exploited by hackers for web attacks.
5. Injection attacks accounted for 20.7%. This type of risks is graded at A1 in the OWASP Top 10 refactored in 2017.
6. Among attacks launched by exploiting known vulnerabilities in servers, most targeted Microsoft IIS (39%), Nginx (30%), and Apache Tomcat (28).
7. 56% of attacks based on vulnerabilities in servers would cause leak of critical information and most exploitable vulnerabilities were found in legacy servers.
8. Among attacks based on known vulnerabilities in frameworks or applications, 94.3% targeted framework programs. Vulnerabilities in Apache Struts 2 were most frequently exploited. For example, the number of attacks exploiting the Apache Struts 2 REST plug-in vulnerability (CVE-2017-9805) hit 335,776 a day at the maximum.
9. While web application attacks taking place in busy hours (9:00–18:00) accounted for 53.6%, those exploiting known web vulnerabilities were often launched in the wee hours or at weekends, which was closely related to the attack method and motive.
10. In China, Beijing and Zhejiang were still among top 3 in terms of both the web attack source and web attack target.
11. Soon after the WebLogic XMLDecoder deserialization vulnerability (CVE-2017-10271) was disclosed, hackers managed to exploit it to infect WebLogic hosts with malicious miner programs. Attackers exploiting this vulnerability can attack both Windows and Linux hosts.

In 2017, a total of 207,000 attacks occurred in China, and the total attack traffic volume reached 640,000 TBytes. DDoS attacks were significantly affected by policies and financial interests.

5. DDoS Attack Trends in 2017

5.1 Attack Count and Peak Traffic

5.1.1 Attack Count and Traffic

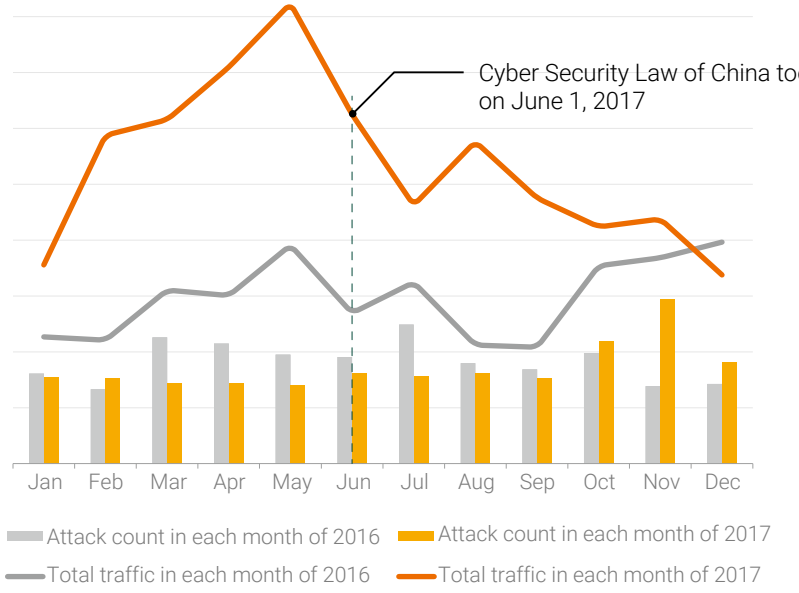
Throughout 2017, a total of 207,000 DDoS attacks happened in China, down 5.8% from 2016. The total volume of attack traffic reached 640,000 TB, up 79.4% from 2016. Obviously, DDoS attacks happened less frequently than in 2016, but generated much more traffic. This is mainly because the scale of DDoS attacks in this year was on the large side. In other words, large and medium-scale attacks rose sharply, while small ones dropped significantly. For details, see section 5.1.2.

In the first half of 2017, the total volume of DDoS attack traffic grew steadily and reached the year's peak in May. From June to December (except August that saw a small fluctuation), it kept sliding until reached the bottom in the fourth quarter. In the latter half of the year, the total volume declined 27.2% compared with the first half. Although the fourth quarter saw more DDoS attacks than the first three quarters, most were small ones and large and medium-scale ones declined significantly (see section 5.1.2), leading to a sudden drop in the total volume of traffic. This was also evidenced by the fact that the average peak size in the fourth quarter was smaller than the first three quarters (see section 5.1.3). We think that this trend of DDoS attacks was due to the following factors:

On the one hand, the *Cybersecurity Law and Measures for the Security Review of Network Products and Services (for Trial Implementation)* came into force on June 1, 2017. They specify legal responsibilities and obligations of government agencies, organizations, and individuals in cybersecurity. The "Legal Liability" chapter imposes higher penalties and more severe punishments for illegal activities, thus increasing the crime cost and constituting a deterrence to cybercrime. Besides, government departments jointly carried out various rectification activities around cybersecurity to clean up the cyberspace and these efforts turned out to be fruitful.

On the other hand, the price of cryptocurrency like Bitcoin soared in the second half of 2017. Deterred by state policies and regulatory controls, hackers on the black market presumably switched high-quality botnet resources at hand from relatively costly DDoS attacks to less costly but more profitable crypto-mining activities. This trend also shows that hackers are obviously profit-driven in their allocation of attack resources.

Figure 5-1 Monthly number and traffic of attacks in 2016 and 2017



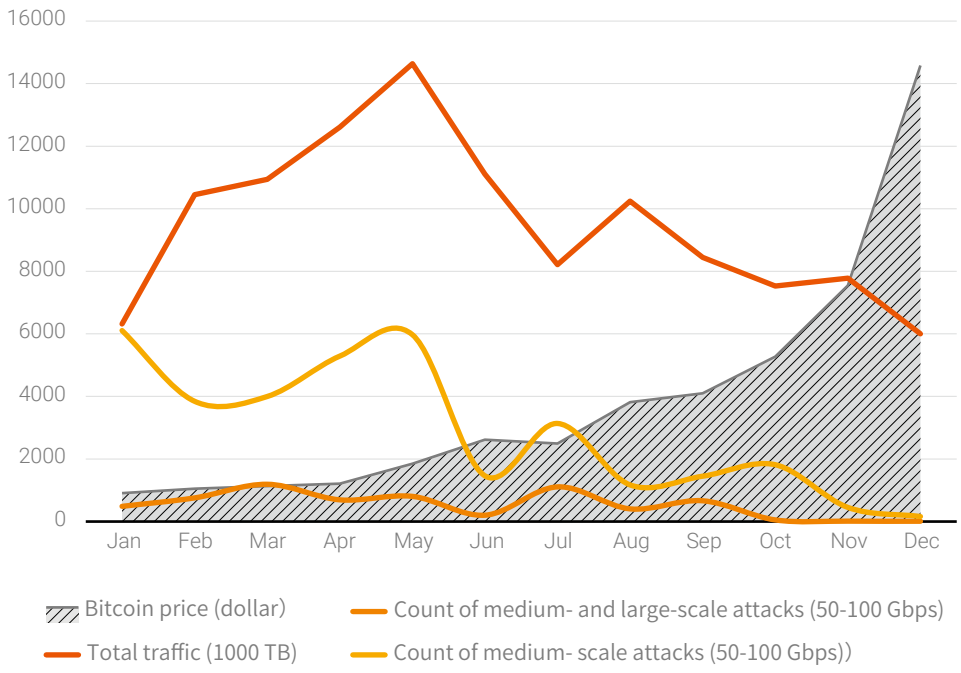
Source: China Telecom YunDi

Figure 5-2 Bitcoin prices in 2017

Source: Bitcoin.com

We had an interesting finding after comparing the trend of Bitcoin prices with that of DDoS attack traffic in 2017: They were inversely proportional to each other, with a correlation coefficient of −0.56. From the perspective of the attack scale, the total traffic of medium-scale attacks was most unproportional to Bitcoin prices, with a correlation coefficient of −0.73. From this relationship, we deduced that hackers on the black market were probably more inclined to allocate botnet resources for DDoS attacks to less costly but more profitable crypto-mining activities.

Figure 5-3 Monthly Bitcoin prices and DDoS attacks in 2017



Source: China Telecom YunDi

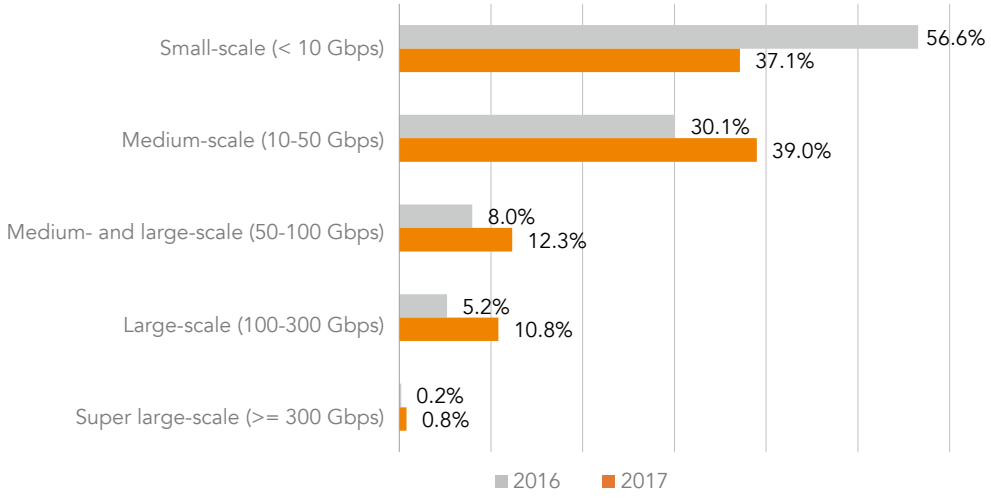
In section 5.2.3, we will analyze medium-scale DDoS attacks from the perspective of the attack source and type that changed from quarter to quarter.

5.1.2 Distribution of Peak Attack Traffic

Compared with 2016, the scale of DDoS attacks in 2017 was on the large side. Specifically, the number of large and medium-scale attacks rose sharply, while that of small ones declined. It is worth noting that super large attacks (≥ 300 Gbps) grew most rapidly by 379% year-on-year. Against this trend of growth, small attacks (< 10 Gbps) dwindled in number by 38%. Attacks of this scale accounted for 56.6% in 2016 and the percentage lowered to 37.1% in 2017, 19.5 percentage points lower.

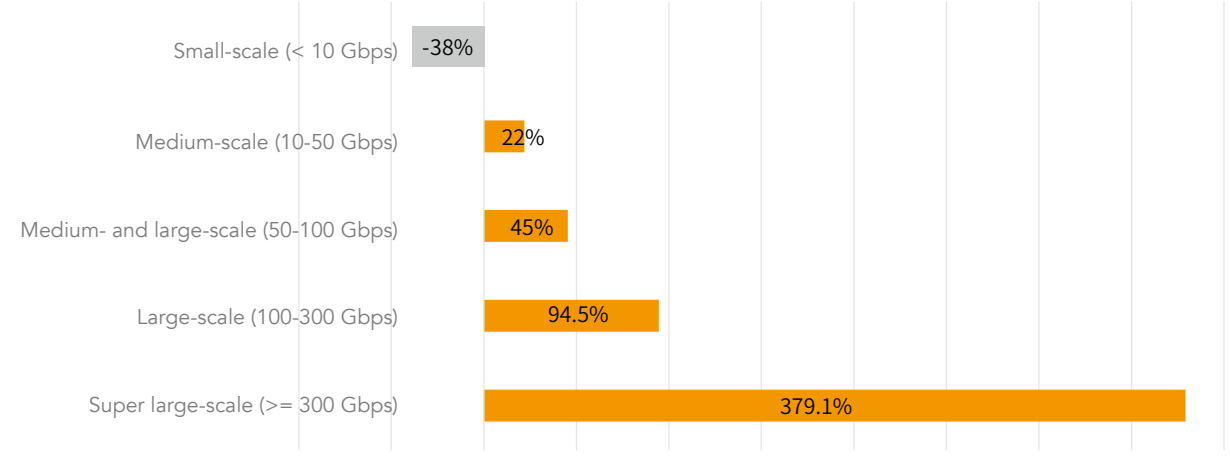
Note: We divide DDoS attacks by peak traffic into small (< 10 Gbps), medium (10–50 Gbps), medium-to-large (50–100 Gbps), large (100–300 Gbps), and super large (≥ 300 Gbps) ones.

Figure 5-4 Proportions of DDoS attacks of various scales in 2017 and 2016



Source: China Telecom YunDi

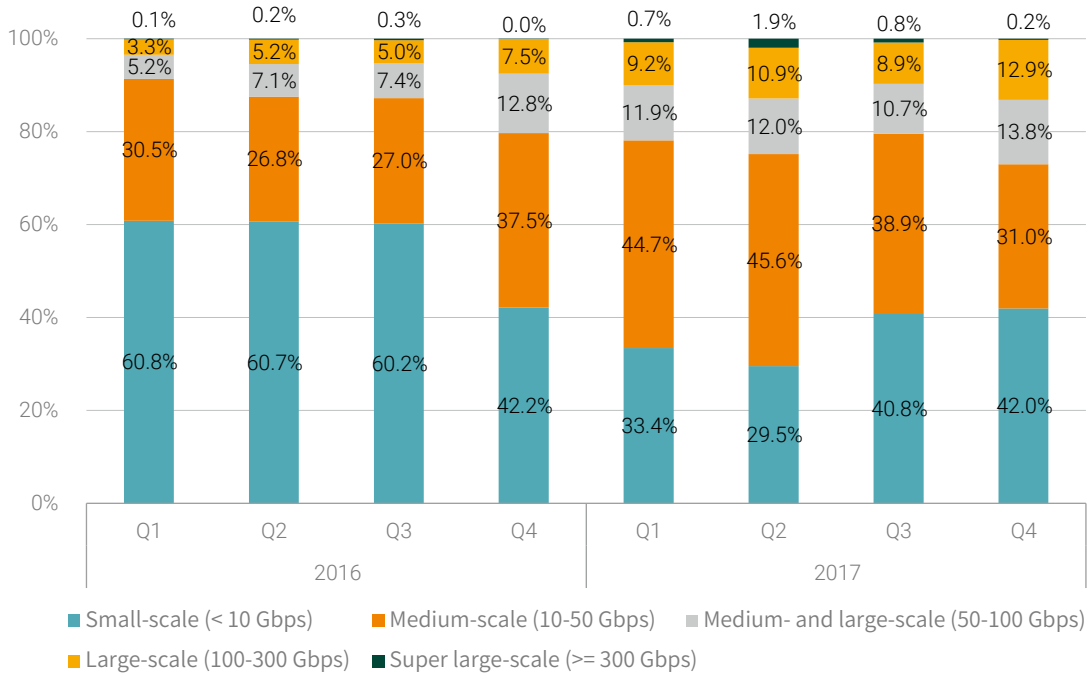
Figure 5-5 Growth (Decline) rate of DDoS attacks of various scales in 2017 and 2016



Source: China Telecom YunDi

Based on the quarterly data of 2017, it is evident that DDoS attacks kept expanding in scale in the first half of the year, but this trend slowed down in the second half. In the first two quarters, large and medium-scale attacks gained momentum for rapid growth. From the third quarter, super large and medium-scale attacks lost momentum, but small ones increased significantly. The contrast between the fourth quarter and the second quarter was sharpest. Compared with the second quarter, the number of medium-scale attacks decreased by 14.6 percentage points and that of super large attacks by 89.5 percentage points, but the number of small attacks increased by 21.5 percentage points in the fourth quarter. For the cause of such a change, see section 5.2.3.

Figure 5-6 Quarterly proportions of DDoS attacks of various scales in 2017 and 2016



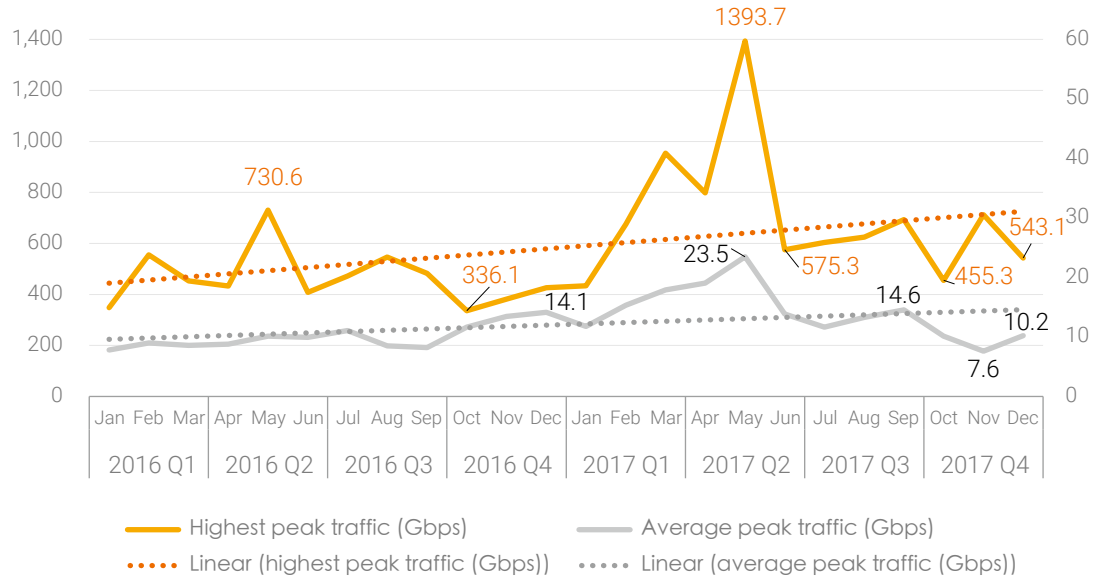
Source: China Telecom YunDi

5.1.3 Maximum/Average Peak Traffic of Individual Attacks

The average peak traffic and maximum peak traffic of individual attacks were both in the upward trend in 2016 and 2017. The average peak traffic was 14.1 Gbps in the entirety of 2017, up 39.1% from 2016. The largest DDoS attack occurred in May, with the traffic peaking at 1.4 Tbps. The average peak traffic in that month also hit the year's record high of 23.5 Gbps.

After a constant growth in a period spanning 2016 and the first two quarters of 2017, the average peak traffic and maximum peak traffic showed a downward trend in the second half of 2017, with the former decreasing 33.7% from the first half of the year. This could be directly attributable to the fact that more small attacks occurred, but much fewer super large and medium-scale attacks were launched, as described in section 5.1.2.

Figure 5-7 Monthly single-attack traffic peak and average attack peak（Gbps）



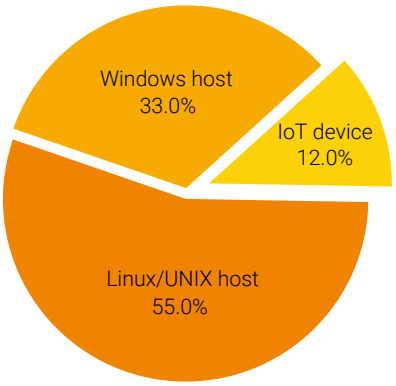
Source: China Telecom YunDi

5.2 Analysis of Attack Sources

5.2.1 Types of Hosts as Attack Sources

We used NSFOCUS Threat Intelligence (NTI) to identify source IP addresses found in DDoS attacks launched in 2017 and had the following finding: Linux/UNIX hosts or servers[4] accounted for 55%, followed by Windows hosts or servers (33%) and IoT devices (12%).

Figure 5-8 Proportions of device types exploited to launch DDoS attacks

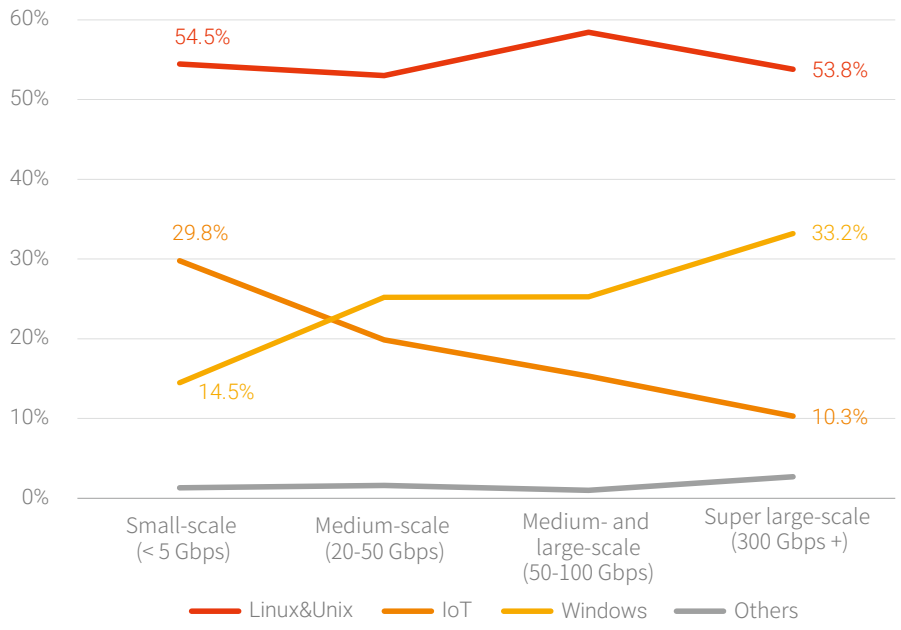


Source: NTI

After grouping these attack sources by attack scale, we found that device types changed with the attack scale, and this phenomenon was especially true for IoT devices and Windows hosts: In small attacks, IoT devices were much more frequently seen than Windows devices; in attacks of the medium scale or above, the proportion of IoT devices declined, but that of Windows hosts increased. Among these Windows hosts, two-thirds were Windows servers. Holistically, Linux/UNIX devices[5] were most common as attack sources, with a proportion of more than 50%, which did not vary much with the attack scale. In this sense, they have become a steady type of "contributors" to DDoS attacks.

4, 5 Here, we mean hosts or servers with Linux/UNIX as the operating system, excluding IoT devices with embedded Linux.

Figure 5-9 DDoS attack source types changing with the attack scale



Source: NTI

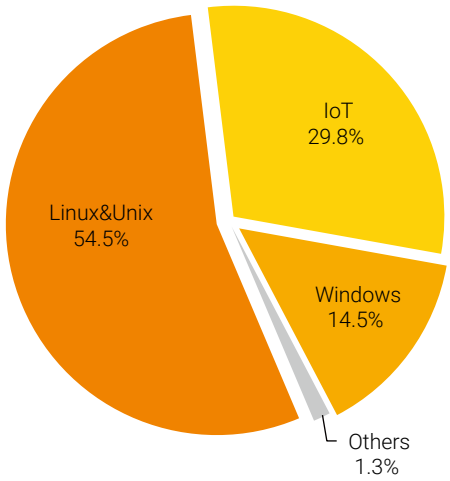
In 2017, about 150,000 independent IP addresses were involved in super large DDoS attacks as attack sources. Linux/UNIX hosts accounted for 53.8%, followed by Windows hosts' 33.2%. IoT devices took up only 10.3%. Moreover, most Linux/UNIX and Windows hosts were servers, nearly half of which were web servers. There were also file storage servers and database servers. We found that some devices ran VMware ESXi Server, which is mainly used for virtualization of cloud-side host resources to achieve flexible allocation of cloud-side server resources to users. This phenomenon also corroborates our viewpoint put forward in NSFOCUS's *2017 H1 DDoS and Web Application Attack Landscape*: Attackers often targeted high-performance, large-bandwidth servers so as to create more powerful, more efficient botnets.

We also found that the change of attack sources with the attack scale was largely due to hackers' decisions on how to allocate botnet resources in DDoS activities. For example, large DDoS attacks often precisely target an organization, paralyzing its business and rendering its services unavailable. Such attacks, once successfully conducted, will bring huge profits to hackers. Therefore, to achieve their purpose more easily, hackers are more inclined to use large-bandwidth, high-performance Windows and Linux hosts as bots to attack targets. Compared with IoT devices, these devices consume large quantities of resources during attacks, which is easy to be detected and then handled by administrators, thus tending to become useless for attackers. For this reason, attackers are more willing to use these bots for more profitable attack activities.

5.2.2 Types of IoT Devices as Attack Sources

In 2017, a total of about 1.3 million independent IP addresses were found in small DDoS attacks as attack sources. Among these sources, Linux/UNIX devices still took up the largest proportion (54.5%), followed by IoT devices (29.8%). This is evidently different from the statistical result of super large attacks. IoT devices involved in small attacks were 19.5 percentage points more than those in super large attacks.

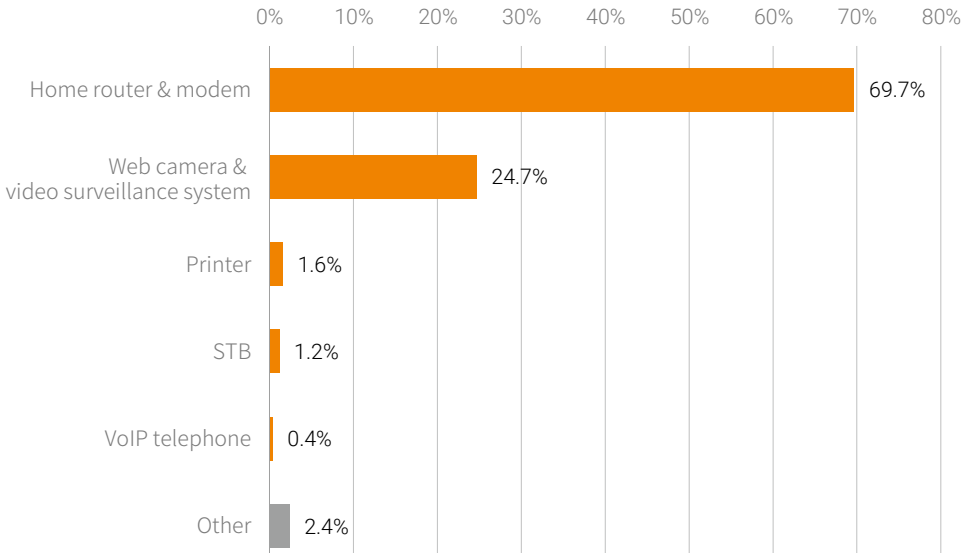
Figure 5-11 Proportions of IoT device types exploited to launch DDoS attacks



Source: NTI

A breakdown analysis of IoT devices involved in small attacks found that home routers and modems accounted for 69.7% and video surveillance devices for 24.7%. Also included were printers, set-top boxes (STBs), and VoIP devices.

Figure 5-11 Proportions of IoT device types exploited to launch DDoS attacks



Source: NTI

Looking further into home routers used as attack sources, we found that some routers and modems were from well-known vendors in China and these devices took up quite a large portion. Moreover, many wireless routers or modems had port 7547[6] publicly available. This is the default port used by TR-069 (also known as Customer-Premises Equipment WAN Management Protocol) or TR-064 (LAN-Side CPE Configuration). TR-069 and TR-064 are respectively used for configuration and management of WAN-side and LAN-side CPE devices such as home routers and modems. However, many of such devices do not restrict the WAN-side use of TR-064. This means that, as long as this port is publicly available, anyone can exploit these vulnerabilities to connect to such CPE devices as home routers and modems. Worse still, this protocol is prone to a command injection vulnerability in NTP server configuration[7]. With this vulnerability, it would not come as a surprise if malicious users take control of numerous home routers worldwide. The outage event affecting about 900,000 customers of Deutsche Telekom at the end of November 2016 was caused by a Mirai variant that exploited vulnerabilities in TR-064 to scan large quantities of home routers. It was reported that 4% to 5% of Zyxel routers broke down[8]. Subsequently, KCOM, TalkTalk (360,000 customers)[9] , and Post Office Broadband (100,000 customers) in the United Kingdom (UK) and Eir [10] in Irelandwere also attacked.

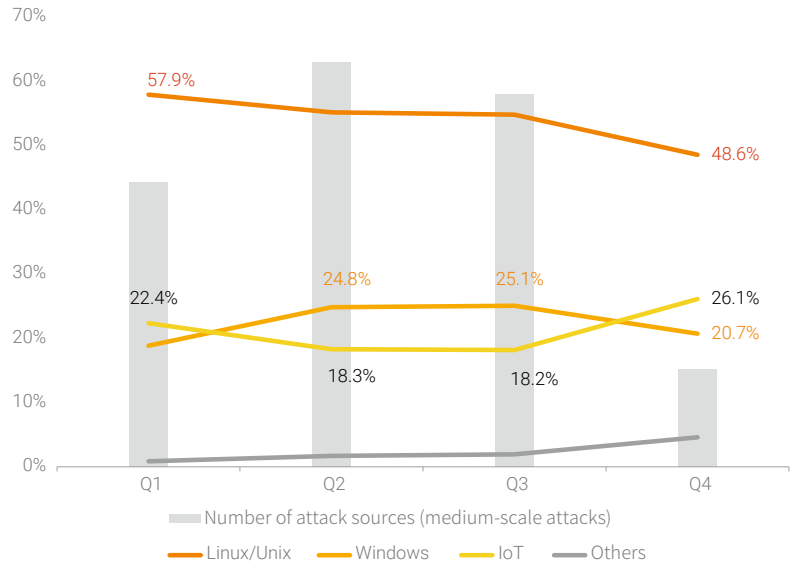
However, this is only a tip of the iceberg. In 2017, more and more botnet malware based on IoT devices emerged, some modified from Mirai of 2016 and some being traditional Linux- and Windows-based botnets with extended infection and control capabilities achieved through the IoT. These malware families are far more powerful than previous ones in terms of infection, propagation, and attack capacities. Besides, they are better at hiding themselves.

5.2.3 Quarterly Statistics of Attack Sources by Number and Type

Based on the findings described in sections 5.1.1 and 5.1.3, we analyzed attack sources quarter by quarter that were involved in medium-scale attacks in 2017. There was a sharp contrast between the fourth quarter and the second quarter. In the fourth quarter, the number of attack sources decreased by 75.8%, mainly Linux/UNIX[11] and Windows hosts. Malicious crypto-miners usually target Windows or Linux servers or hosts. For example, the Bondnet botnet takes Windows servers as its main target because these devices generally have more computing resources than small home appliances[12]. Of course, there are a small portion of crypto-miner botnets that are based on IoT devices. At a time when the price of cryptocurrency like Bitcoin soars, it is natural for hackers to allocate these high-quality resources to crypto-mining for more profits.

6 http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/
7 https://www.exploit-db.com/exploits/40740/
8 http://toutiao.secjia.com/new-mirai-attack-germany-telecom
9 https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.htm
10 https://motherboard.vice.com/en_us/article/nz7ky7/hackers-say-knocking-thousands-of-brits-offline-was-an-accident-mirai
11 Here, we mean hosts or servers with Linux/UNIX as the operating system, excluding IoT devices with embedded Linux.
12 http://safe.zol.com.cn/638/6388907.html

Figure 5-12 Proportions of different sources (number and type) of medium-scale DDoS attacks



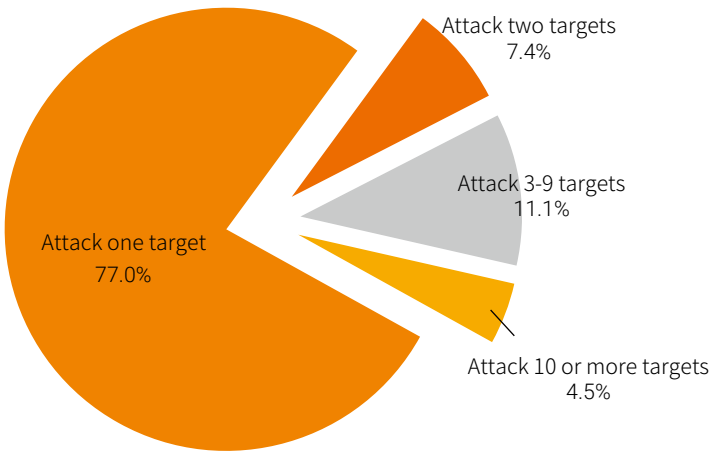
Source: NTI

5.2.4 Target Scope and Reputation of Source IP Addresses

In 2017, among all DDoS attack sources, 23% attacked two or more targets.

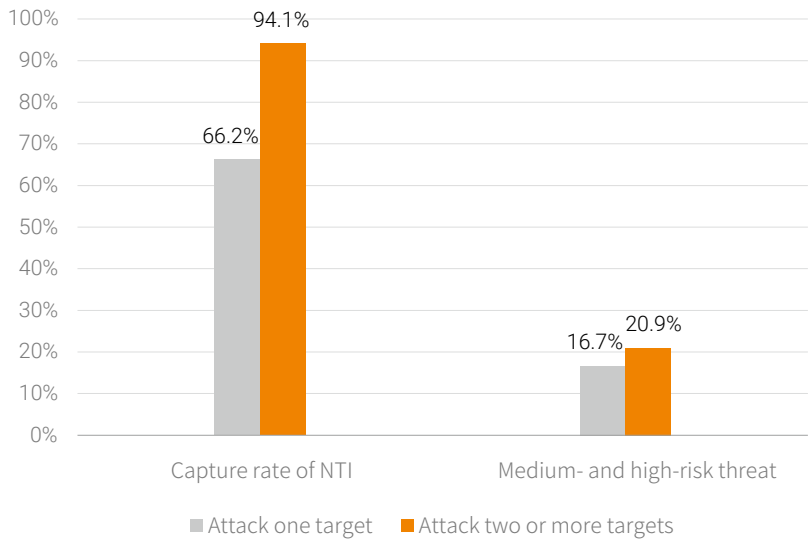
The more targets an IP address attacks, the more active and threatening this IP address is. Among source IP addresses attacking two or more targets, 94.1% can be found on NTI, of which 20.9% are labeled as medium-risk or high-risk. Web application attack sources, which are analyzed in a subsequent section, vary from DDoS attack sources in the capture rate and risk levels. For details, see section 7.6.

Figure 5-13 Proportions of source IP addresses differentiated by the number of targets



Source: NTI

Figure 5-14 Proportions of source IP addresses with different capture rates and risk levels



Source: NTI

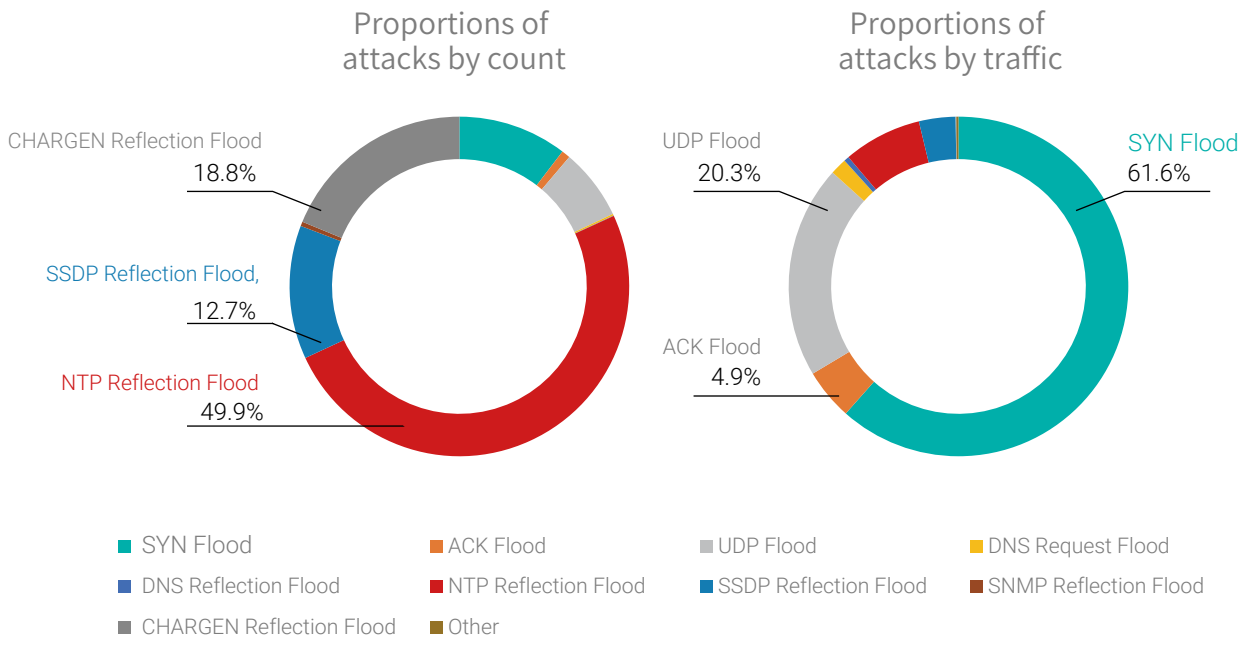
5.3 Attack Type Analysis

5.3.1 Attack Type Distribution by Count and Traffic

In 2017, global statistics reveal that the top 3 DDoS attack types by count were still reflection attacks: NTP reflection flood attacks, SSDP reflection flood attacks, and CHARGEN reflection flood attacks. These three types of attacks accounted for 81.4% in total, almost flat with 2016 and slightly lower than the first half of 2017. This is in line with our view in the 2016 report that reflection DDoS attacks will persist for a long time.

From the perspective of traffic volume, the proportion of UDP flood attacks continues decline, and that of SYN flood attacks continues to grow (61.6%, 12.5% higher than 2016). This is mainly attributed to the significant increase of medium- and large-scale SYN flood attacks (for details, see section 5.3.2).

Figure 5-15 Percentages of various types of DDoS attacks by count and total traffic

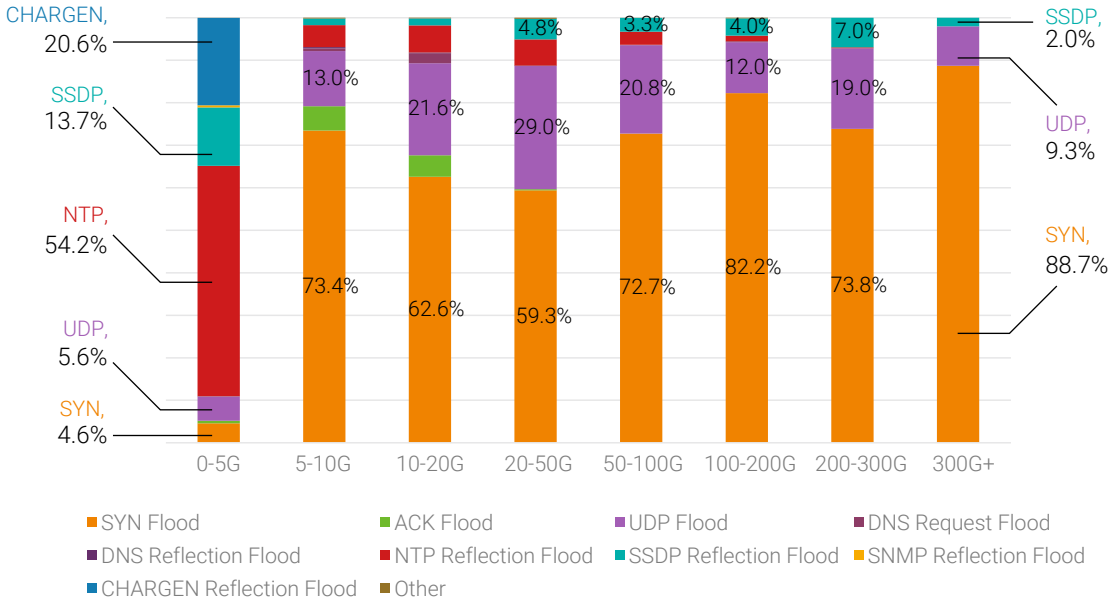


Source: NSFOCUS ATM

5.3.2 Attack Type Distribution in Traffic Segments

In 2017, DDoS attack presents a more complex trend. Compared with 2016, SYN flood attacks make up a larger share in each peak traffic segment. Particularly, the proportions are quardrupled in medium- and large-scale attacks in particular. Such a remarkable increase is primarily due to the emergence of large SYN packets (1514-byte).

Figure 5-16 DDoS attack type distribution in traffic segments



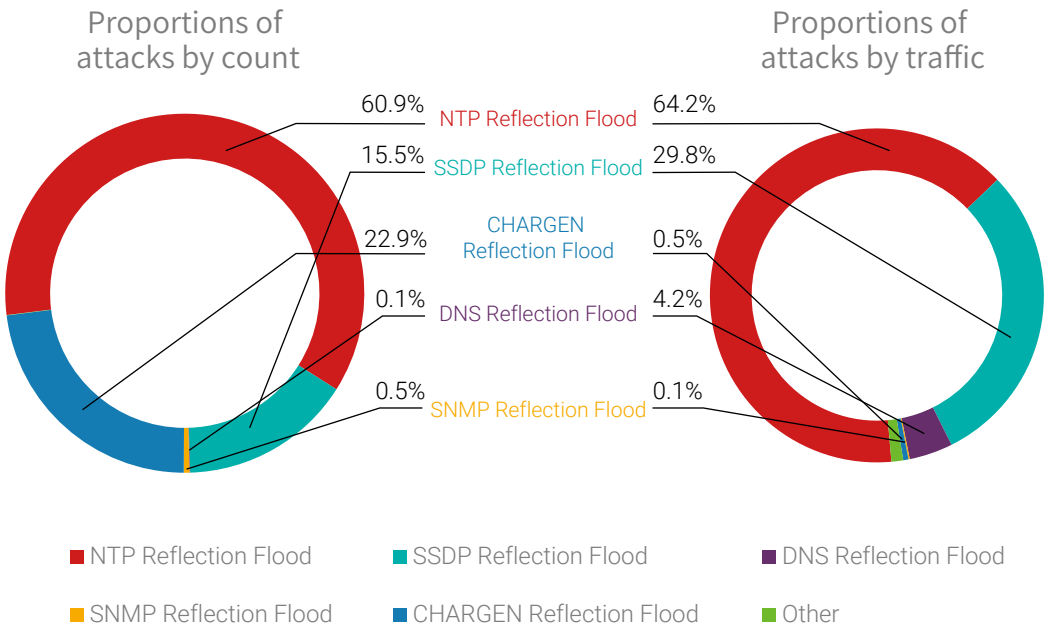
Source: NSFOCUS ATM

5.4 Reflection Attacks

5.4.1 Eased Traditional Reflection Attacks Represented by NTP

For distributed reflection DoS (DRDoS) attacks in 2017, the attack type distribution by count and traffic is as shown in the following figure. NTP reflection flood attacks take the first place in both dimensions, accounting for 60.9% and 64.2% respectively. The number and amplification factor of reflectors are two major factors for an attacker to choose a reflection attack type. Since numerous NTP servers with public IP addresses are available in the Internet and NTP reflection attacks have an amplification factor of 556.9, NTP reflection attacks have been prevalent in recent years.

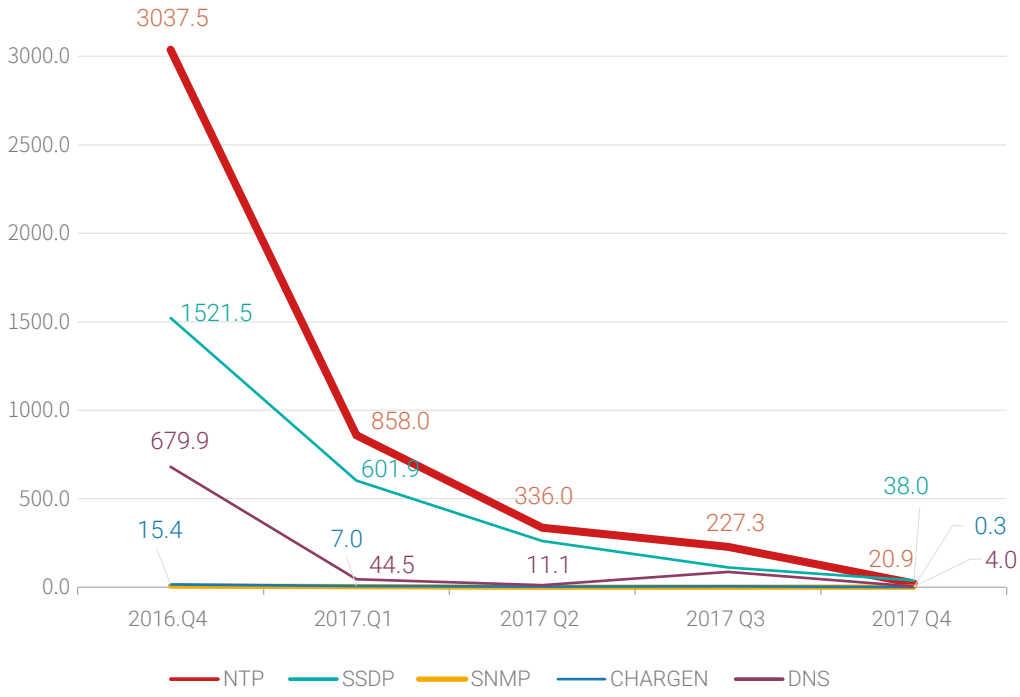
Figure 5-17 Type distribution of reflection attacks by count and total traffic



Source: NSFOCUS ATM

However, from the perspectives of total traffic, attack scale (peak traffic), and number of active reflectors involved, these common types of reflection attacks are trending down in 2017. The total traffic of reflection attacks decreases by 71% in 2017 Q1, compared with 2016 Q4.

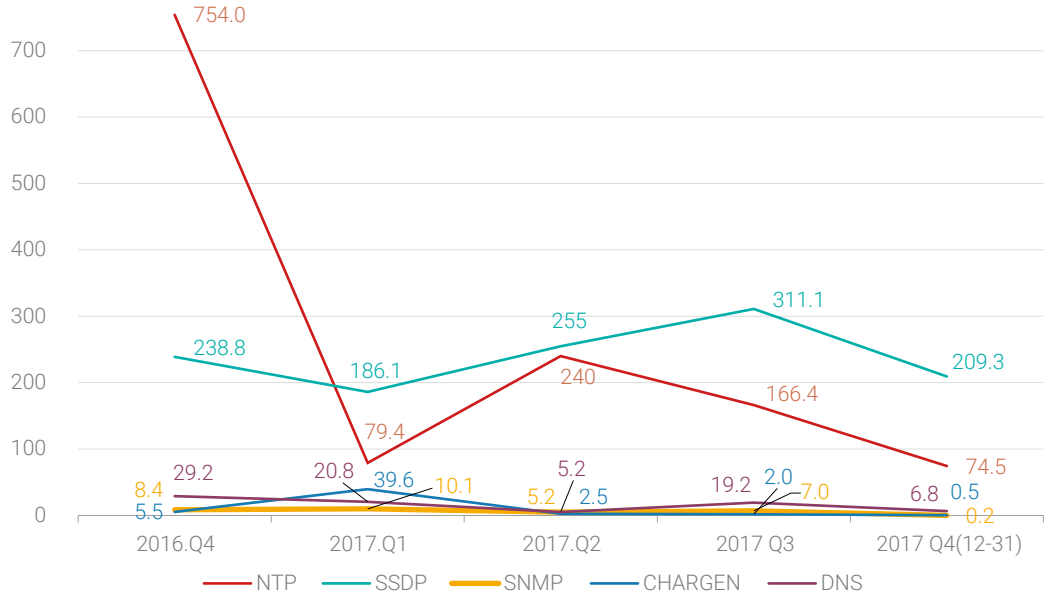
Figure 5-18 Quarterly trend of total traffic of various reflection attack types (TBytes)



Source: NSFOCUS ATM

The year 2017 sees a decline trend in the scales (peak traffic) of all common types of reflection attacks. While the peak traffic of some reflection attack types increases slightly in 2017 Q2 and Q3, but the value in Q4 lower than that in the same period in 2016.

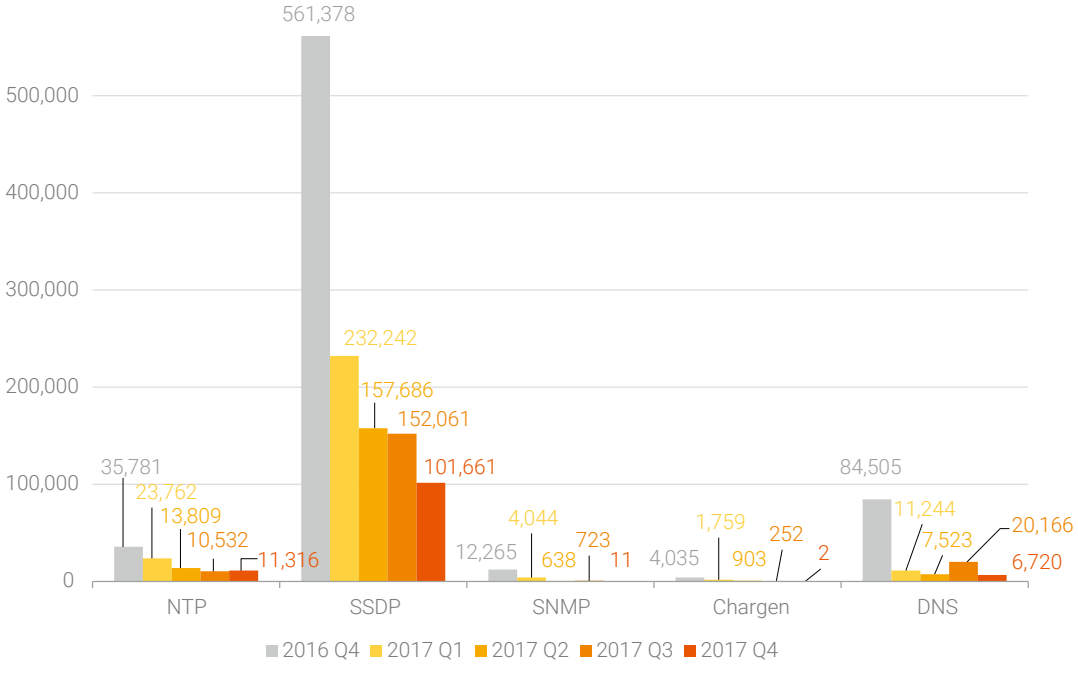
Figure 5-19 Quarterly trend of single-attack peak traffic of various reflection attacks（Gbps）



Source: NSFOCUS ATM

In 2017, reflectors used in the common types of reflection attacks are on the decline.

Figure 5-20 Quarterly trend of numbers of active reflectors involved in various types of reflection attacks



Source: NSFOCUS ATM

The decline in available reflectors accounts for the decrease in the total traffic and attack scale of those common reflection attacks. On the one hand, since these types of reflection attacks have long raged on the Internet, both corporations and individual users are well aware of harms caused by them, and most servers with known vulnerabilities are patched or upgraded or have unnecessary service disabled. On the other hand, attackers have been continuously seeking for new cheaper and more efficient attack tools or approaches. For example, new reflection attacks with high amplification factors, as well as attacks conducted by IoT botnets.

5.4.2 New Memcached Reflection Attack Rushing in with Record-Setting Peak Traffic of 1.35 Tbps

According to our monitoring data, common types of reflection attacks are easing in 2017, such as NTP, SSDP, CHARGEN, and DNS. While people are about to relax their vigilance on reflection attacks, a new type of reflection attack, Memcached, came into the spot light at the beginning of 2018. On March 1, 2018, Akamai claimed that its customer suffered a Memcached DRDoS attack with record-setting peak traffic of 1.35 Tbps[13], just a few days after the record reached 270 Gbps[14] and then 500 Gbps[15]. The record is doubled in just a few days, and the frequency of such attacks also booms. NSFOCUS issued a warning for Memcached DRDoS in the first place[16], and together with YunDi of China Telecom, released an analysis report of Memcached DRDoS[17].

Memcached is a high-performance caching system for open source distributed memory object and is mainly used to improve the scalability of web applications. It can effectively solve many problems of big data caches and is widely used worldwide. Memcached stores small pieces of data based on the key-value of the memory and uses the data to complete database calls, API calls, or page renderings. Attackers make use of the key-value function to create a large-flow Memcached reflection attacks. This will be described later in details. The following table from US-CERT[18] lists the amplification factors for various reflection attacks. Memcached reflection attacks are much more damaging than just other reflection attacks in terms of amplification factor, and data provided by US-Cert show that it achieves an astonishing 51,000x magnification.

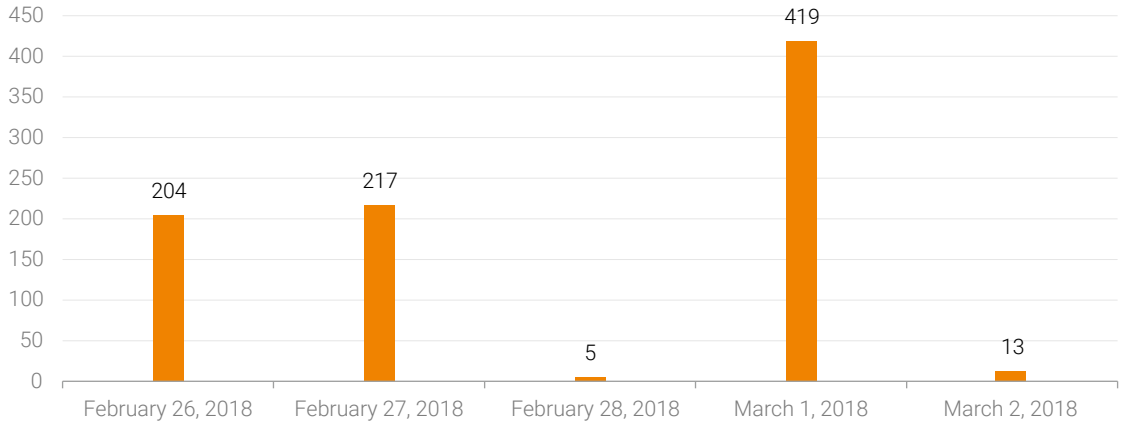
13 https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html
14 https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/
15 https://www.arbornetworks.com/blog/asert/memcached-reflection-amplification-description-ddos-attack-mitigation-recommendations/
16 http://blog.nsfocus.net/memcached-ddos/
17 http://blog.nsfocus.net/memcached-drdos-analysis/
18 https://www.us-cert.gov/ncas/alerts/TA14-017A

Table 5-1 Amplification factors for various reflection attacks

Targeted Protocol of Reflection Attacks	Bandwidth Amplification Factor
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP	56 to 70
TFTP	60
Memcache	10,000 to 51,000

According to China Telecom YunDi, attack monitoring data show that in as short as 5 days – from Monday to Friday (February 26 to March 2 at 06:00), there have been 79 cases using the Memcached protocol amplification attacks around the world. The highest daily sum total of attack traffic reached 429 TB.

Figure 5-21 Daily sum total of Memcached DRDoS attack traffic（TBytes）

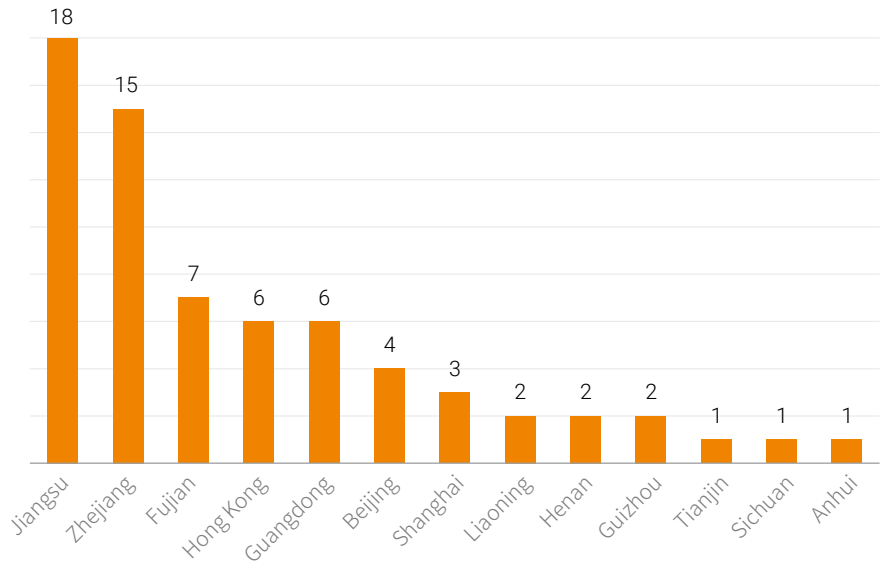


Source: China Telecom YunDi

Among them, there are 68 attacks targeting Memcached in China, with attacks being frequent seen in Jiangsu and Zhejiang provinces. The maximum single-attack against China peaks 505 Gbps. The longest attack took place on March 1, lasting 1.2 hours, with a total attack traffic of 103.8 TBytes.

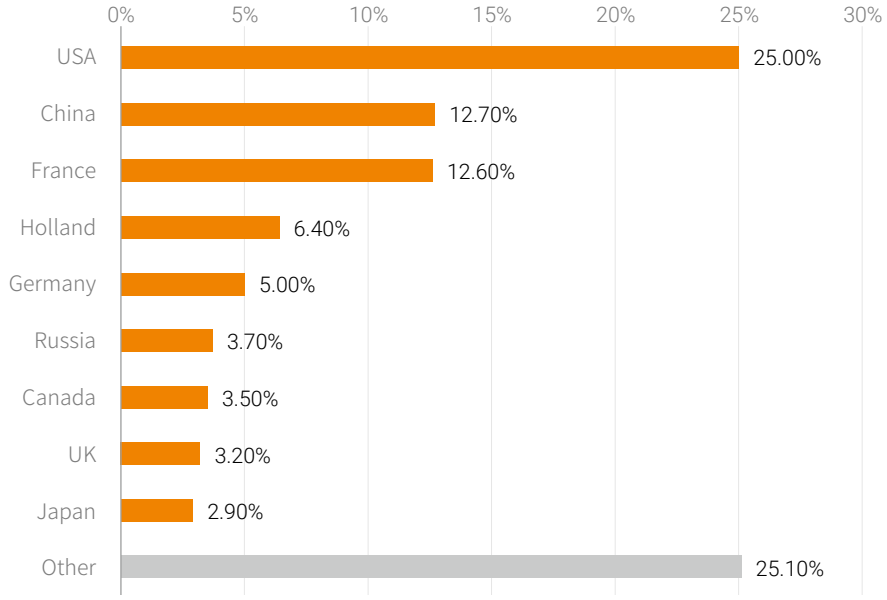
According to the root-cause analysis result, a total of 3,790 Memcached servers are being utilized worldwide to participate in these Memcached reflection amplification attacks. These sources of reflection are distributed across 96 countries around the world. Among them, the United States accounted for 1/4 of the world total. Distributed Memcached servers in China ranked second, accounting for 12.7%. The share of provinces in China is shown as follows. Guangdong, Beijing and Zhejiang are top 3.

Figure 5-22 Numbers of Memcached DRDoS attacks detected in provinces and municipalities in China



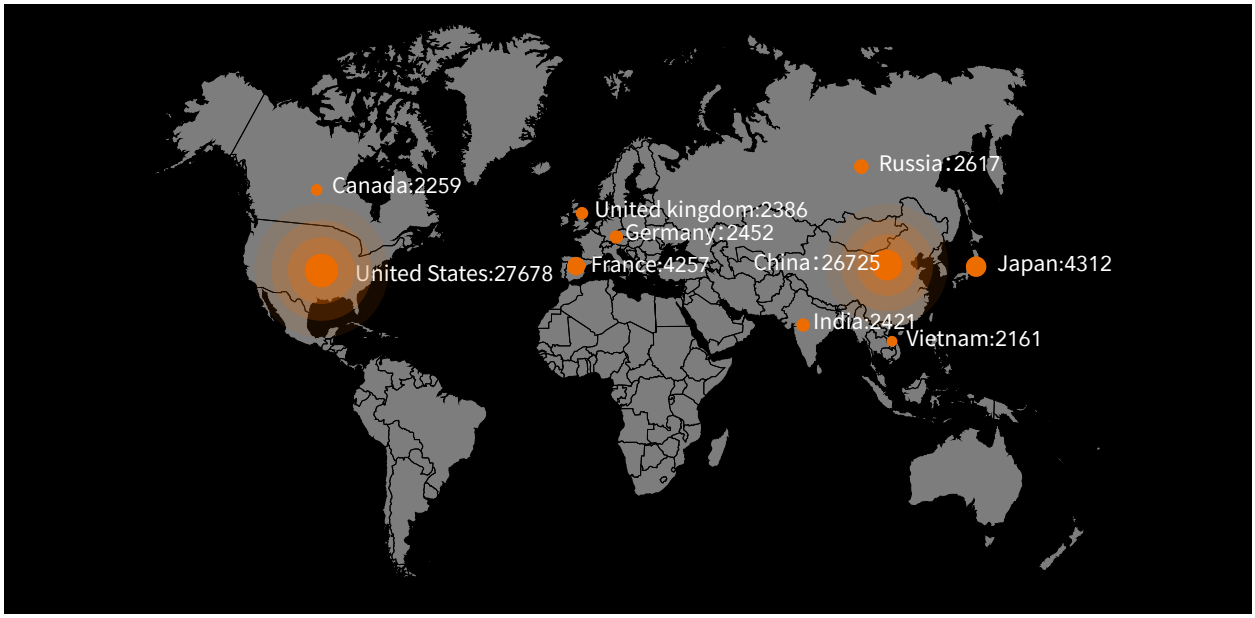
Source: China Telecom YunDi

Figure 5-23 Global distribution of sources of Memcached DRDoS attacks



Source: China Telecom YunDi

The statistics of the NSFOCUS Network Threat Intelligence (NTI) show that there are 104,506 Memcached servers worldwide at risk of being utilized. Geographically, Memcached servers are the most available in the United States, followed by China.



Source: NTI

These active Memcached reflectors provide a powerful tool for building super volume DRDoS attacks. If no counter measures are taken in time, the number of attacks based on Memcached is expected to continue to increase, with serious consequences.

In terms of impact, all Internet businesses may become targets of Memcached DRDoS attacks. Broadband service providers suffer from large traffic attacks, resulting in the outbound bandwidth fully occupied and the normal business not accessible; on the other hand, enterprise internal Memcached systems may be used by criminals and become an accomplice. We urge customers in various regions and sectors to keep high vigilance against Memcached-based DRDoS attacks which may have a direct impact on servers or compromise information security by covering other attacks. For recommendations on protection and hardening against Memcached-based DRDoS attacks, see *Deep Analysis Of Memcached Large DRDoS Attacks*[19].

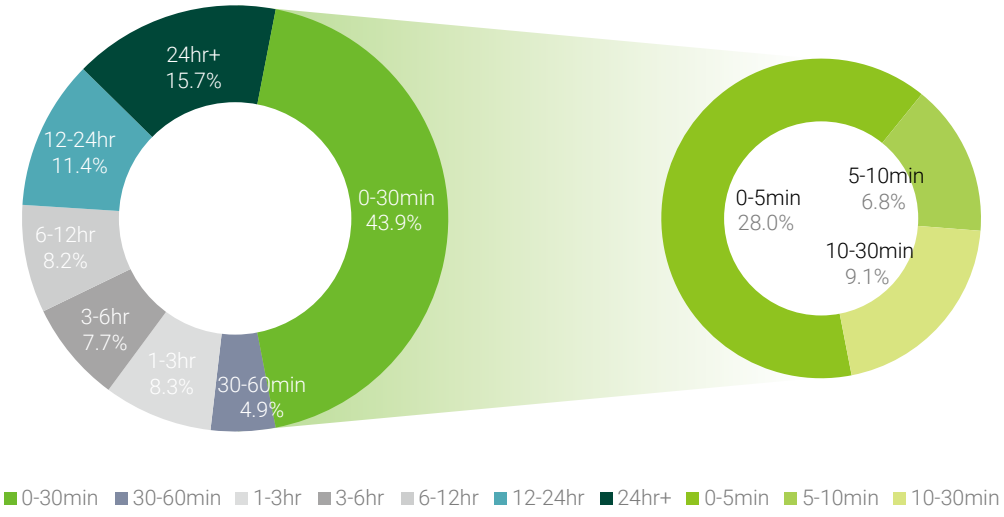
19 http://blog.nsfocusglobal.com/categories/emergency-response/deep-analysis-of-memcached-large-drdos-attacks-china-telecom-damddos-nsfocus-jointly-released/

5.5 Attack Duration

5.5.1 Attack Duration Distribution

In 2017, attacks lasting more than 24 hours increase, while those lasting less than 30 minutes decrease slightly but still dominate. In 2017, the latter account for 43.9% of all DDoS attacks, 7.5% lower than that in 2016; the former continuously increase and account for 15.7%, 5% higher than that in 2016. As the servitization and industrialization of DDoS attacks, along with numerous hacked IoT devices becoming bots around the world, the cost of conducting a DDoS attack is reduced significantly. Hackers are capable of larger and longer DDoS attacks with the same cost, leading to the increase of long-lasting attacks.

Figure 5-24 Attack duration distribution



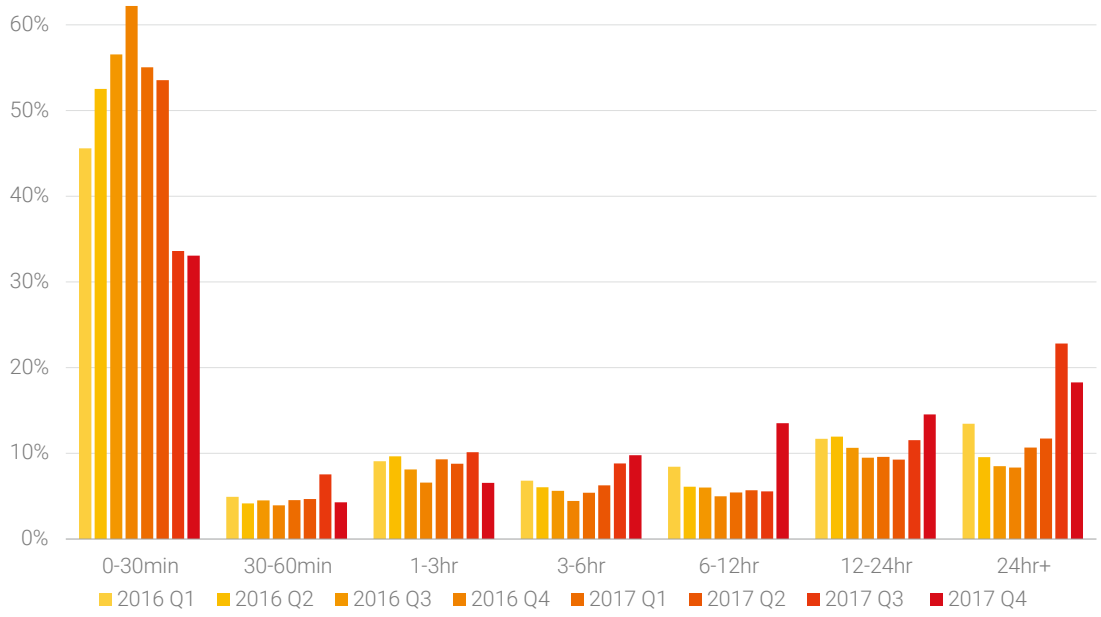
Source: NSFOCUS ATM

5.5.2 Trend of Attack Duration

The year 2017 sees an upward trend of attacks lasting more than 3 hours.

According to our long-term monitoring of attack duration, for attacks lasting less than 30 minutes, the proportion falls from more than a half in 2017 Q2 to about one third in 2017 Q3 and Q4; for attacks lasting more than 3 hours, the proportion keeps increasing since 2017 Q1.

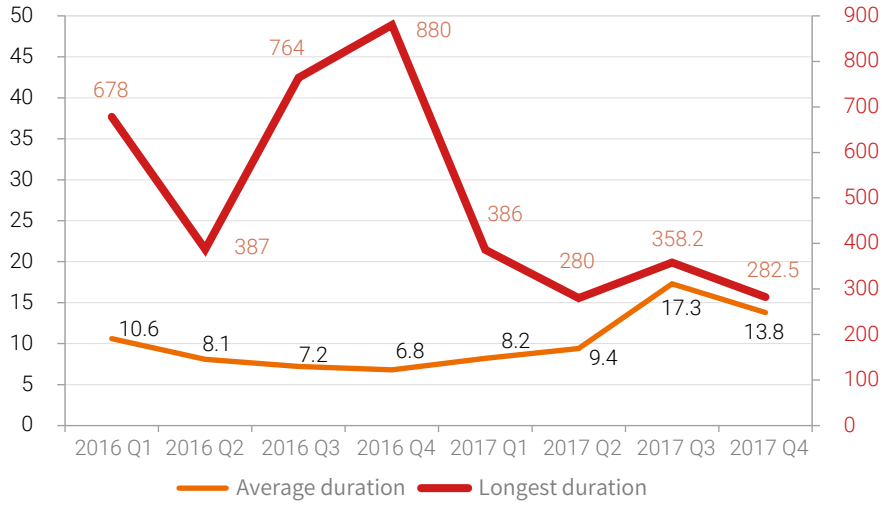
Figure 5-25 Quarterly distribution of attack duration



Source: NSFOCUS ATM

The average attack duration is 12 hours in 2017, about 1/3 longer than that in 2016. The longest attack duration in each quarter of 2017 decreases compared with that in the same period of 2016. The most long-lasting DDoS attack we monitored in 2017 persisted for 16 days plus 2 hours (386 hours).

Figure 5-26 Average and longest attack duration in each quarter (hour)

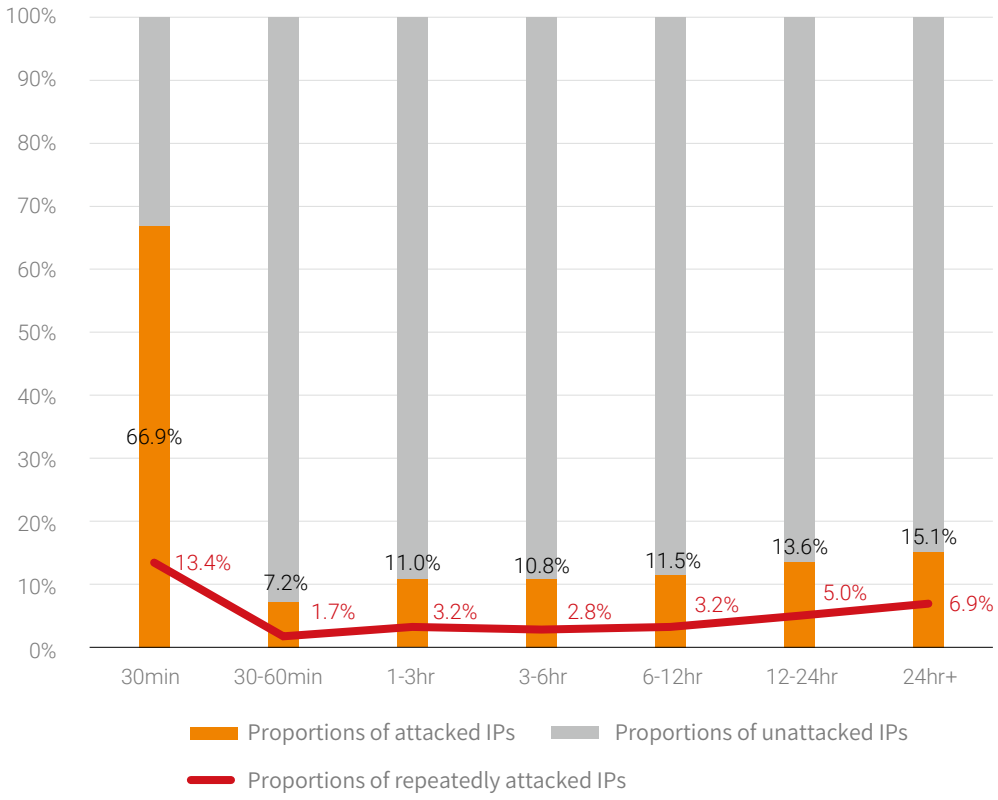


Source: NSFOCUS ATM

5.5.3 Relationship Between Attack Frequency and Duration

Successfully and repeatedly attacked target IP addresses are most frequently seen in attacks lasting less than 30 minutes.

Figure 5-27 Relationship between attack frequency and duration



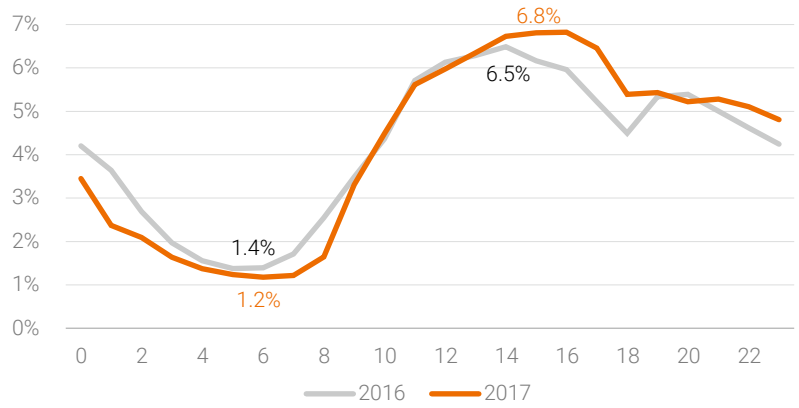
Source: NSFOCUS ATM

5.6 Attack Time Profile

5.6.1 Round-the-Clock Attack Distribution

Round-the-clock attack distribution shows no obvious difference between 2016 and 2017. In 2017, the proportion increases for attacks occurring in besiness and leisure hours (10:00 am to 10:00 pm); accordingly, the proportion decreases for attacks occurring in sleeping hours. The trend is also seen in Internet service visits in 2017: upward in besiness and leisure hours, and downward in sleeping hours. This means that attackers use that trend to achieve higher efficiency and greater influence, by conducting DDoS attacks during busy hours. In 2017, DDoS attack occurring in busy hours (10:00 am to 10:00 pm) accounts for 75.7%.

Figure 5-28 Round-the-clock attack distribution in 2016 and 2017

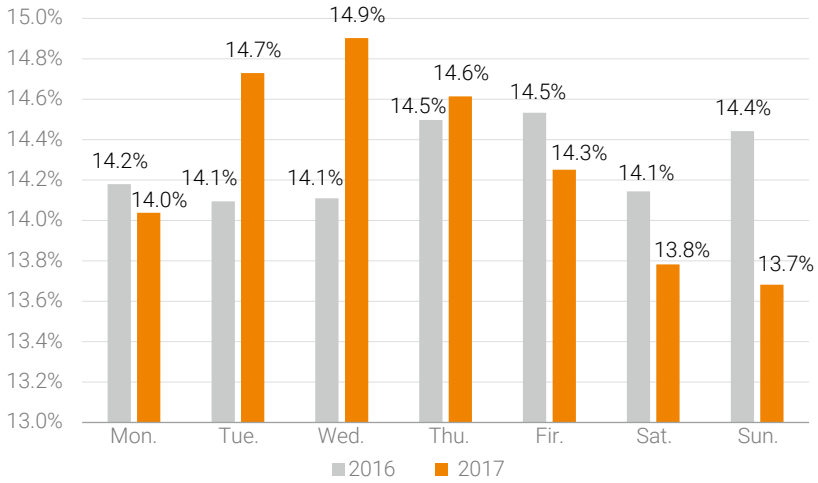


Source: China Telecom YunDi

5.6.2 Round-the-Week Attack Distribution

In 2017, the proportion increases for attacks occurring in weekdays, and decreases for those occurring in weekends, compared with 2016. In short, DDoS attacks occur more often in weekdays than in weekends.

Figure 5-29 Round-the-week attack distribution in 2016 and 2017



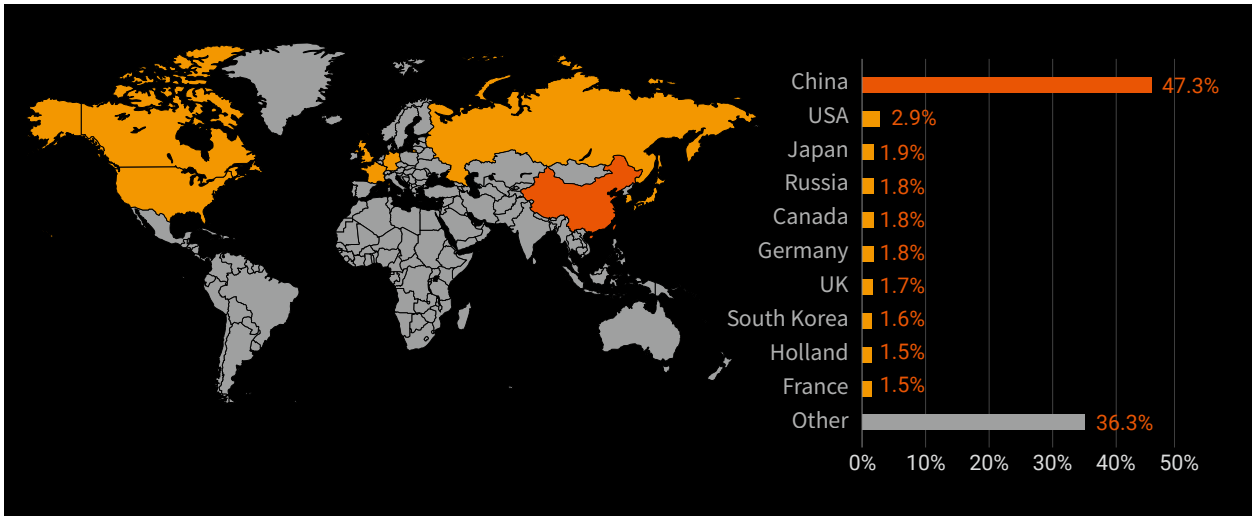
Source: China Telecom YunDi

5.7 Geographical Distribution of Attacks

5.7.1 Geographical Distribution of Attack Sources

According to our statistics, in 2017, China still houses the most controlled attack sources, which accounted for 47.3% of the global total. USA, Japan, Russia, Canada, and Germany each accounts for about 2%. Other attack sources are distributed in developed countries in a roughly even manner.

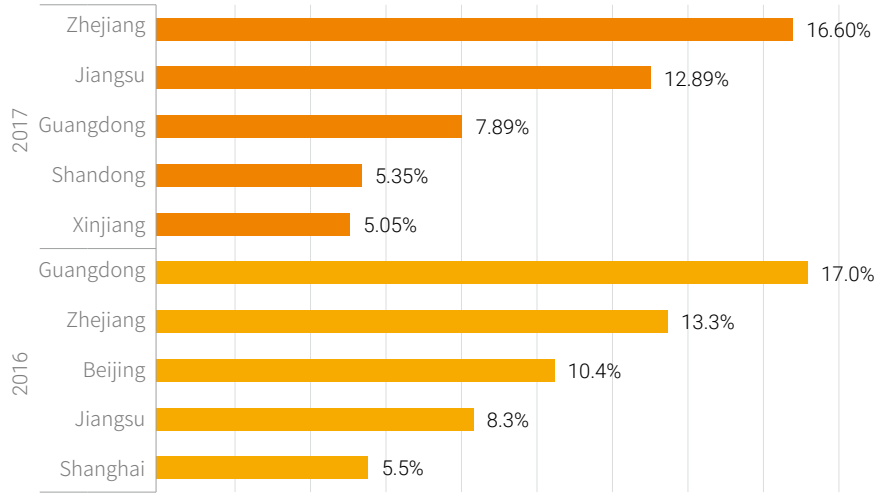
Figure 5-30 Top 10 attack source countries



Source: NSFOCUS ATM

In 2017, DDoS attack sources mainly locate in coastal and northwestern provinces. The top 5 provinces are Zhejiang, Jiangsu, Guangdong, Shandong, and Xinjiang, accounting for 47.88% in total. Shandong and Xinjiang are included in the top 5 list for the first time.

Figure 5-31 Top 5 attack source provinces in 2016 and 2017

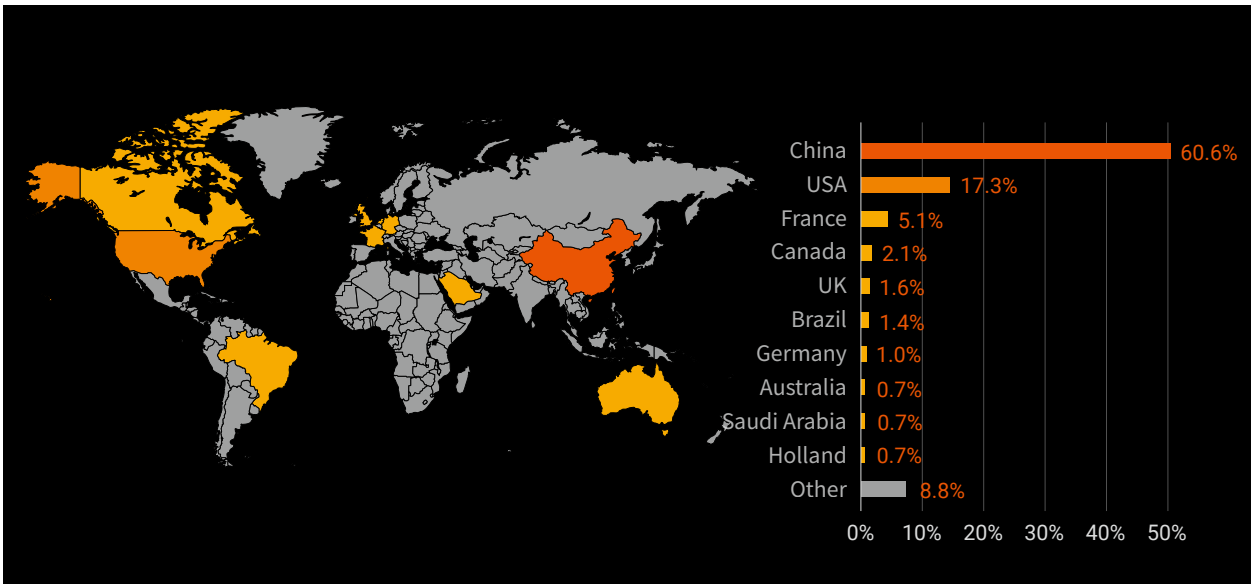


Source: China Telecom YunDi

5.7.2 Geographical Distribution of Attack Targets

In 2017, China suffers 60.6% of global DDoS attacks, taking the first place and followed by USA and France. In total, the top 3 countries meet 83% of all DDoS attacks in 2017, 10.8% lower than 2016.

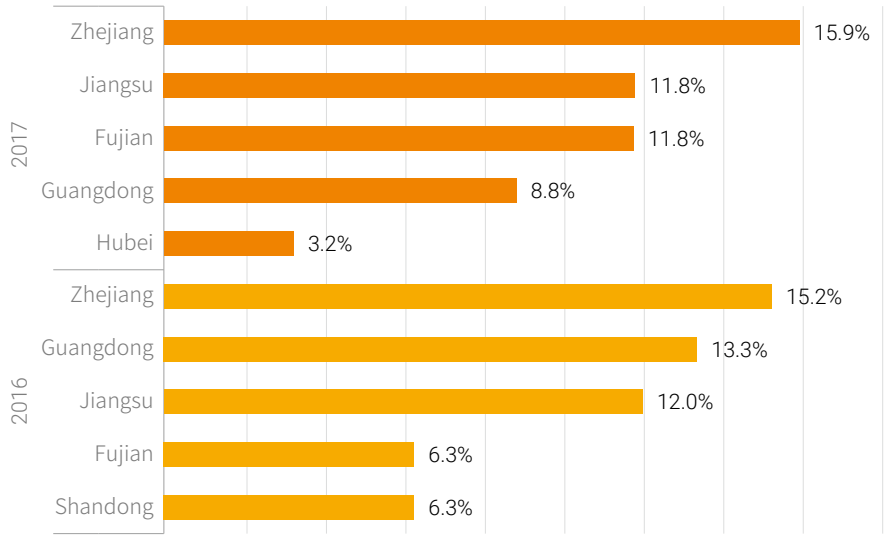
Figure 5-32 Top 10 attack target countries



Source: NSFOCUS ATM

The mid-eastern coastal provinces have always been the most favored targets of DDoS attacks. In 2017, Zhejiang, Jiangsu, Fujian and Guangdong totally suffered 51.5% of all attacks targeting China. In 2017, Zhejiang is still the most attacked province, and Fujian is included in top 3 for the first time.

Figure 5-33 Top 5 attack target provinces in 2016 and 2017



Source: China Telecom YunDi

6. IoT Botnets

IoT botnets are constantly upgraded in propagation, infection, and attack capabilities, and the potential target platforms continues to expand. The threats brought by IoT botnets will further expand.

6.1Trends of IoT Botnet Evolvement

6.1.1 Upgraded Way Of Infection: From Weak Password Cracking to 0-Day Vulnerability Exploitation

IoT botnets boomed in 2016. Most of IoT botnets, represented by Mirai, infected IoT devices by cracking weak Telnet and SSH passwords. In November 2016, a Mirai variant attacked many home routers by exploiting the TR-064 router vulnerability, knocking 900,000 customers at Deutsche Telekom offline. One after another, British Kcom, TalkTalk (360,000 customers)[20], Post Office Broadband (100,000 customers), and Irish telco Eir were affected[21].

2017 sees more variants developed based on IoT botnets. Most of them are integrated with more complicated vulnerability scan and exploitation capabilities, and some of them even infect IoT devices via 0-day vulnerabilities. It is astonishing that the black market update botnet vulnerabilities so quickly.

For example:

As we know for now, IoTroop[22] [23] has exploited more than 15 vulnerabilities in GoAhead, D-link, TP-link, Netgear, AVtech, MikroTik, Linksys, Synology and other products. GoAhead itself contains 5 of the 15 vulnerabilities, CVE-2017-8225/CVE-2017-8224/CVE-2017-8223/CVE-2017-8222/CVE-2017-8221.

Okiru/Sator[24] exploits a 0-day vulnerability (CVE-2017-17215) in some Chinese-brand wireless routers, which allows remote attackers to execute arbitrary code by sending malicious packets to port 37215. Besides that, Okiru/Sator exploits a remote code execution vulnerability (CVE-2014-8361) in the miniigd SOAP service of Realtek SDK (an SDK development toolkit issued by Realtek). This vulnerability allows remote attackers to execute arbitrary code by sending specially crafted NewInternalClient requests. Affected products are mainly multiple models of Dri series home router provided by D-link.

In addition to cracking weak Telnet/SSH passwords, Persiriai [25]and Gafgyt [26] are capable of infecting IoT devices via vulnerability exploitation. For example, Gafgyt[27] was initially found hacking IoT devices by scanning and cracking weak Telnet/SSH passwords. Then, a later version was found being integrated with modules of scanning and exploiting vulnerabilities in Netcore routers.

6.1.2 Further Expansion of The Infection Platform: Able To Spread Across Platforms

1.Traditional Windows- and Linux-based botnets start targeting IoT devices.

Open-source Mirai sharply increases IoT botnet variants. Traditional Windows-based botnet families quickly

20 https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.html
21 https://motherboard.vice.com/en_us/article/nz7ky7/hackers-say-knocking-thousands-of-brits-offline-was-an-accident-mirai
22 https://research.checkpoint.com/new-iot-botnet-storm-coming/
23 http://blog.netlab.360.com/iot-reaper-a-quick-summary-of-a-rapid-spreading-new-iot-botnet/
24 http://www.freebuf.com/articles/paper/158464.html
25 https://www.incapsula.com/blog/from-mirai-to-persirai.html
http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/
26 http://toutiao.secjia.com/gafgyt-iot-malware
27 http://www.freebuf.com/articles/terminal/148668.html

evolve into IoT platforms after witnessing the quantity, scale and damage of IoT[28] . Typical representatives are Jenki and Typhoon families. Till now, the Jenki family possesses controlled-end trojons across Windows, Linux, and IoT platforms.

2. Windows-based trojons are used for cross-platform propagation.

A Mirai-based variant, BKDR_MIRAI.A[29] , uses a Windows-based trojon to propagate and infect across Windows and IoT platforms. An IoT-oriented Mirai malware will be planted upon the detection of a Linux-based system, while a Windows trojon will be installed upon the detection of a Windows-based system and continues to scan new infection targets. The trojan can also identify host software, such as the database system of MS SQL or MySQL. It will create a new account with admin privileges, capable of conducting arbitrary database operations.

It is unspecified that whether this variant is linked to Mirai.Nov[30]. At the beginning, Mirai.Nov install malware via the Windows-based Dofloo botnet[31].

3. Compatibility with more IoT platforms.

As discovered in a Mirai.Nov sample, its controlled-side trojan is compatible with armv5l, armv6l, i586, i686, mipsel, mips, x86_64, and powerpc architectures on which most IoT systems are built. This provides an architecture compatibility basis for large-scale expansion of botnet in the future.

mirai.mipsel-v1-1031	2017/11/3 11:15	MIPSEL-V1-1031...	43 KB
mirai.x86_64-v1-1031	2017/11/3 11:14	X86_64-V1-1031...	34 KB
mirai.i686-v1-1031	2017/11/3 11:14	I686-V1-1031 file	29 KB
mirai.i586-v1-1031	2017/11/3 11:12	I586-V1-1031 file	28 KB
mirai.armv6l-v1-1031	2017/11/3 11:09	ARMV6L-V1-103...	53 KB
mirai.armv5l-v1-1031	2017/11/3 11:08	ARMV5L-V1-103...	30 KB
mirai.powerpc-v1-1031	2017/11/3 11:07	POWERPC-V1-1...	31 KB
mirai.mips-v1-1031	2017/11/3 11:07	MIPS-V1-1031 ...	43 KB

Amnesia[32] supports 10 IoT platforms:

- armv4l
- armv5l
- i386
- m68k
- MIPS
- MIPSEL

28 https://mp.weixin.qq.com/s/SFYHBaju-CkNTpoViValbg
29 http://blog.trendmicro.com/trendlabs-security-intelligence/mirai-widens-distribution-new-trojan-scans-ports/
30 http://www.freebuf.com/articles/web/153689.html
31 http://www.freebuf.com/articles/paper/159800.html
32 http://get.cyberx-labs.com/radiation-report

- PowerPC-440fp
- SPARC
- x86_64

6.1.3 Being More Covert: Use of More Covert Scanning Techniques and Sandbox Techniques

1. More covert scanning techniques.

1）BKDR_MIRAI.A[33] isolates the scanning and cracking module from bots. Then it performs bot infection[34] via multiple approaches of the Windows-based trojon, including SQL blind injection and brute-force cracking (SSH/ Telnet).

2）Mira.Nov [35]also isolates the scanning module from bots so that bots are mainly responsible for conducting DDoS attacks and C2 interactions. Doing this can lower the odds that bot code is detected during vulnerability scanning and weak (Telnet/SSH) password cracking, and quickly reuse latent bots. However, the botnet's expansion pace will be lowered, due to the lack of capability of scanning bot clusters.

3）IoTroop[36] [37] will proactively restrain the scanning speed to reduce the risk of being detected or identified.

2. Use of traditional virtualization techniques to avoid sandbox detection

Researchers found that IoT/Linux-based Amnesia/Tsunami use virtual machine evasion techniques[38], which are often used in Windows- and Android-based malware to evade detection and analysis by a sandbox. The Amnesi malware will check whether a host is running in a sandbox, for example, by detecting VMware or QEMU environment based on virtual devices. If yes, the malware will delete all files in this host.

6.1.4 Constant Upgrade of Arsenals: Integration of Reflection Attack Capabilities

IoT/Linux-based malicious botnets not only possess application-layer attack capabilities, but are also integrated with reflection attack capabilities. According to analysis, IoT_Reaper is integrated with about 100 public DNS servers, capable of conducting DNS reflection attacks. As estimated, a single C2 has infected 20,000 devices, with 2,000,000 more potential targets. Gafgyt [39] is also capable of conducting UDP reflection attacks.

There are an enormous amount of such IoT/Linux devices. Once a certain number of available reflectors are integrated, such DDoS reflection attack will cause much greater damage than traditional reflection attacks. Also, the attack cost will be reduced significantly. Besides the amount of devices controlled by the botnet, the attack scale is directly related to reflector types and the amount of available reflectors. For examples, NTP reflectors have the greatest amplification factor, while SSDP reflectors are most available.

33 http://blog.trendmicro.com/trendlabs-security-intelligence/mirai-widens-distribution-new-trojan-scans-ports/
34 https://securelist.com/newish-mirai-spreader-poses-new-risks/77621/
35 http://www.freebuf.com/articles/web/153689.html
36 https://research.checkpoint.com/new-iot-botnet-storm-coming/
37 http://blog.netlab.360.com/iot-reaper-a-quick-summary-of-a-rapid-spreading-new-iot-botnet/
38 https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
39 http://toutiao.secjia.com/gafgyt-iot-malware

6.1.5 Black Market More Energetic in Scrambling for IoT Botnet Resources

1. Traditional botnets are extending IoT infection capabilities.

Some traditional Windows- and Linux-based botnets extend IoT infection capabilities, becoming more energetic in scrambling for IoT botnet resources. Statistics[40] show that 24% of hosts in Mirai botnets have the same IP addresses used by Gafgy or Bashlite in attacks. Such a high proportion indicates that different malware families target the same vulnerable IoT devices.

2. Some botnets "harden" IoT devices to prevent similar malware from infection.

After infecting an IoT device, much malware will purposely disable some ports that are often used by other malwares to infecting the device. This is mainly to prevent the loss of control on the device after a similar malware infects the device again via the ports. For example, malware Hajime, under the cloak of IoT device protection, will disable ports 23, 7547, 5555, and 5538 after infecting an IoT device[41].

```
int iptables_1A5F4()
{
  int v0; // r5@1
  int v2; // [sp+0h] [bp-5Ch]@2
  int v3; // [sp+40h] [bp-1Ch]@1
  signed int v4; // [sp+44h] [bp-18h]@1
  signed int v5; // [sp+48h] [bp-14h]@1
  signed int v6; // [sp+4Ch] [bp-10h]@1

  v3 = 23;
  v4 = 7547;
  v5 = 5555;
  v6 = 5358;
  v0 = 0;
  do
  {
    sub_1F0A0(
      (int)&v2,
      64,
      (int)"iptables -A INPUT -p tcp --destination-port %d -j DROP",
      *(int *)((char *)&v3 + v0 * 4));
    ++v0;
    sub_23CFC(&v2);
  }
  while ( v0 != 4 );
  sub_23CFC("iptables -D INPUT -j CWMP_CR");
  return sub_23CFC("iptables -X CWMP_CR");
}
```

```
BEDE5CCB  00 B0 AF 02 00 7B 1D 00  00 69 70 74 61 62 6C 65  .....{...iptable
BEDE5CDB  73 20 2D 41 20 49 4E 50  55 54 20 2D 70 20 74 63  s -A INPUT -p tc
BEDE5CEB  70 20 2D 2D 64 65 73 74  69 6E 61 74 69 6F 6E 2D  p --destination-
BEDE5CFB  70 6F 72 74 20 37 35 34  37 20 2D 6A 20 44 52 4F  port 7547 -j DRO
BEDE5D0B  50 00 00 00 00 00 00 00  00 17 00 00 00 7B 1D 00  P............{..
0123DFFF  01                                               .
```

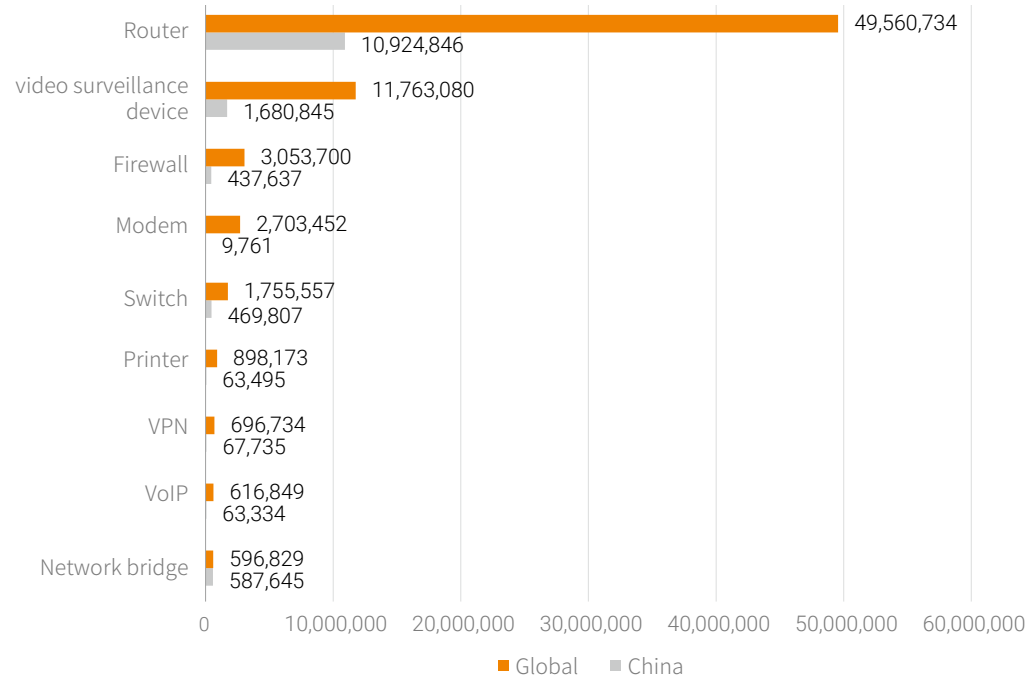
Similar to Hajime, BrickerBot[42] , alleging to do righteous actions, will harden an infected IoT device by rewriting the Flash memory, to prevent another malware's infection. The author of BrickerBot declared that BrickerBot had hardened 10,000,000 IoT devices since the kickoff of its "Internet Chemotherapy" programs in November 2016.

40 https://mp.weixin.qq.com/s/SFYHBaju-CkNTpoViValbg
41 http://zhishi.secjia.com/pdf/770583325.pdf
42 https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

6.1.6 More and More Threats from IoT Botnets

In the architecture of IoT, terminal devices and traditional datacom devices are both indispensable. The security posture and trend of both types of devices are key factors for sustainable and stable IoT development. In IoT security events, attackers often obtain exposed IP addresses and ports by entire-network scanning and then perform targeted intrusion and control. Therefore, the amount, types, and distribution of exposed IoT devices have become important indications of potential IoT security risks.

Figure 6-1 Exposure of IoT devices globally and in China (Unit)



Source: 2017 IoT Security Report

After collecting and analyzing data, we list in Figure 6.1 several IoT devices that are heavily exposed, as well as their amounts.

Globally, due to the great amount of deployed datacom devices, such devices are much more exposed in IoT than IoT terminal devices. The amounts of most common routers and firewalls exposed reach 49,560,000 and 3,050,000 respectively, taking the first and third places. As video surveillance devices are extensively employed in IoT, the amount of exposed video surveillance devices reaches 11,760,000, taking the second place.

In China, exposed routers (10,920,000), video surveillance devices (1,680,000), and firewalls (400,000) take the top three places.

Routers are most common devices in network infrastructure. Hidden security issues in routers should never be ignored. Since routers in carrier networks have clear requirements for deployment and configurations to prevent exposure, most exposed routers in the network are home routers.

Assuming that 1% of exposed home routers are infected, then about 110,000 home routers in China are at risk of becoming bots. Usually, the uplink bandwidth is 12.5 Mbps for a home router. Then a maximum of 1.3 Tbps DDoS attack traffic can be generated.

Amount IoT terminal devices, webcams are mostly seen in daily life. Due to low prices and easy deployment, they are extensively employed in IoT. At present, new botnets http81 and IoT_reaper are both focusing on webcams.

Assuming 1% of webcams in Chine are infected, then about 16,800 video surveillance devices are at risk of becoming bots. Since a surveillance device sending 1080P videos require at least 40 Mbps of uplink bandwidth, a maximum of 672 Gbps attack traffic can be generated.

In fact, the current security status of IoT devices is rather worrying and related security issues are seldom fixed in time. This provides a far higher chance of infection than 1% for these devices. These resources, once controlled by cyber criminals, will pose inestimable dangers.

6.2 Comparative Analysis of Popular IoT Botnets

6.2.1 Overview

As the most familiar botnet in recent years, Mirai controlled an astonishing amount of 600,000 vulnerable IoT devices at its peak. Criminals usually gain profits through botnets by providing rental and sales of DDoS attack services as well as blackmailing target services. As the rise of Bitcoin price reached 1600% in 2017, we witnessed that botnets became an important resource for mining bitcoins. This is the major cause to the rapid development of new botnets in 2017.

This section summarizes new botnets in 2017, and performs thorough comparative analysis from the perspectives of hosting platform, propagation methods, and potential threats.

6.2.2 Comparative Analysis of Hosting Platforms

By comparing seven new botnets in 2017, we find that their infection targets have extended from webcams to common home devices such as routers and set-top boxes. Hajime and BrickerBot can even propagate among any network terminal devices.

The hosting platforms divided into two types: IoT-based and Linux-based platforms. This is because IoT mainly adopts IoT- and Linux-based platforms that requiring low hardware performance, due to the constraints of costs and application scenarios.

Table 6-1 Comparison of hosting platforms

Botnet Type	Infected Hardware Type	Hosting Platform
IoT_reaper[43] [44]	1. Routers: Dlink, Netgear, Linksys 2. Webcam: Goahead, JAWS, AVTECH 3. NVR: Vacron	IoT/linux
Persirai[44] [45]	Webcam	IoT
Hajime[47]	Any Internet device	IoT
Gafgyt[48]	Routers: Netcore, Netis	IoT/Linux
Amnesia[49]	Webcam, DVR	IoT
Rowdy[50]	Set-to-top box	Linux
BrickerBot[51]	Webcam, set-to-top box, and others	Linux

6.2.3 Comparison of Propagation Methods

The infection methods of new botnets are not limited to Mirai's way of simply cracking weak passwords. Various exploitation of vulnerabilities and backdoors also increases the speed and scale of botnet development. Meanwhile, criminals continue to add new vulnerabilities to maintain the sustainable development of their botnets.

The major propagation method is automatic scanning of specific Telnet ports. However, new methods of probing application layers such as HTTP become a development trend.

Table 6-2 Comparison of propagation methods

Botnet Type	Infection	Propagation
IoT_reaper	Vulnerability exploitation, with 15 vulnerability integrated	Automatic Telnet scanning
Persirai	1. Exploitation of default and weak passwords 2. Vulnerability exploitation, with 3 vulnerability integrated	Web scanning
Hajime	1. Exploitation of default and weak passwords 2. Exploitation of RCE vulnerability	1. Search of DHT network 2. Arris cable modem 3. Exploitation of TR-069 vulnerability
Gafgyt	Exploitation of igdmptd vulnerability on Netcore routers	Proactively scanning port 53413
Amnesia	Exploitation of RCE vulnerability	Scanning of keywords in HTTP response
Rowdy	Exploitation of default and weak passwords	Automatic Telnet scanning
BrickerBot	Exploitation of default and weak passwords	Automatic Telnet scanning

43 https://research.checkpoint.com/new-iot-botnet-storm-coming/
44 http://blog.netlab.360.com/iot-reaper-a-quick-summary-of-a-rapid-spreading-new-iot-botnet/
45 https://www.incapsula.com/blog/from-mirai-to-persirai.html
46 http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/
47 http://blog.nsfocus.net/hajime-sample-technical-analysis-report/
48 http://toutiao.secjia.com/gafgyt-iot-malware
49 https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
50 http://blog.nsfocus.net/iot-set-top-box-malware-rowdy-network-analysis-report/
51 https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

6.2.4 Comparative Analysis of Potential Threats

Infections by new botnets have magnitudes varying from 10,000 to 10,000,000, depending on the security state of target devices as well as the infection skills.

Threats of botnets are mainly presented as DDoS attacks. The maximum attack bandwidth is estimated to reach the Terabyte level. While the major attack types are traditional TCP, UDP, and CC attacks, some botnets are able to conduct complicated and efficient CC attacks in Lua execution environment.

Particular specification should be given to BrickerBot. Initially founded for so-called "Internet chemotherapy" rather than conducting malicious DDoS attacks. "Internet chemotherapy" means taking vulnerable devices offline, thereby forcing device owners to update firmware. However, the industry and experts generally believe that it performs permanent denial of service (PDoS) on IoT devices.

Table 6-3 Comparison of potential threats

Botnet	Infection Magnitude	Potential DDoS Threat
IoT_reaper	10,000 active infected nodes per day	1. 100 Gbps attack bandwidth 2. Complicated and efficient CC attacks in Lua execution environment
Persirai	120,000 infected nodes 12,000 active infected nodes per day	1. 120 Gbps attack bandwidth 2. Major attack types being SSDP and UDP
Hajime[52]	60,000 to 80,000 active infected nodes per day	1. 600 to 800 Gbps attack bandwidth 2. No attack type till now
Gafgyt	1.5 million devices globally, and 1.2 million devices in China	1. Maximum 15 Tbps attack bandwidth globally 2. Major attack types being UPD, TCP, and HTTP
Amnesia	2,300 infected devices out of 230,000 vulnerable devices	1. 230 Gbps attack bandwidth 2. Major attack types being UPD and HTTP
Rowdy	3000 bots in China	1. 30 Gbps attack bandwidth 2. Major attack types being SYN, ACK, HTTP, DNS, GRE
BrickerBot	More than 10 million of IoT devices	PDoS on IoT devices

52 https://sec.xiaomi.com/article/33

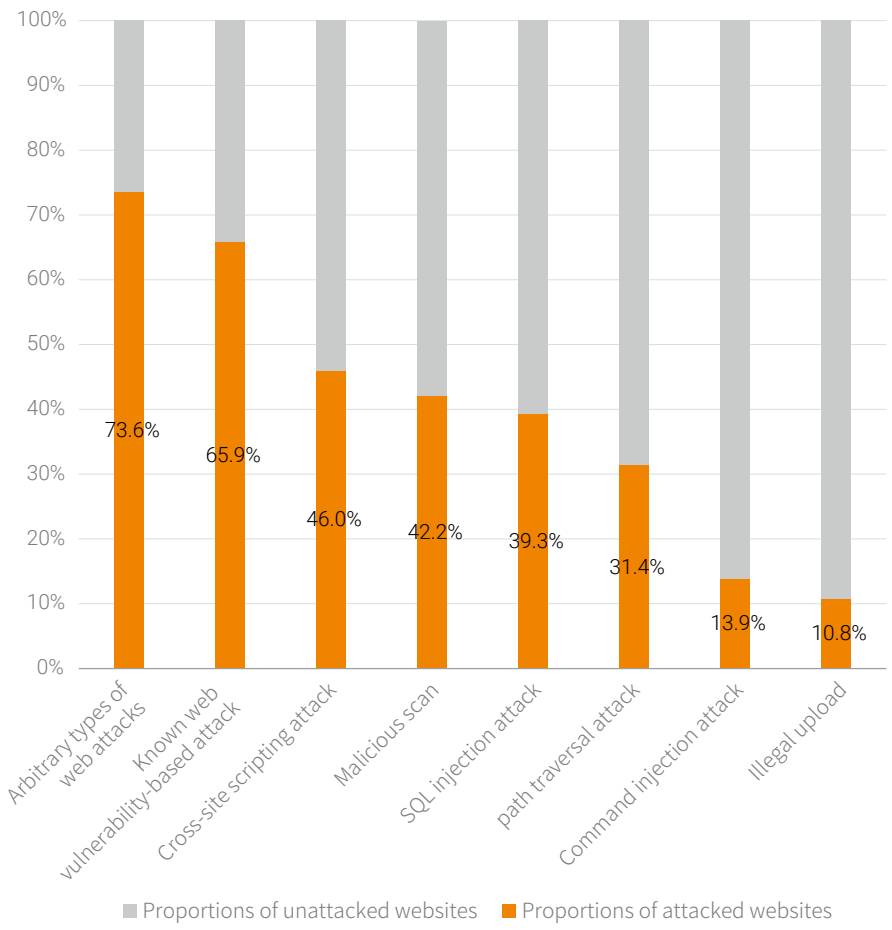
XSS scripting attacks, accounting for 37.7%, are the most commonly seen web attacks, followed by injection attacks accounting for 20.7%.

7. 2017 Web Application Attack Landscape

7.1 Attacked Websites

Among websites under our protection in 2017, 73.6% were hit by web application attacks. In terms of the scope of attack targets, attacks based on web vulnerabilities (including known vulnerabilities in web servers and web frameworks) came first, targeting 65.9% websites. Following this type of attacks were XSS attacks, malicious scans, and SQL injection, respectively striking 46%, 42.2%, and 39.3% of websites. In the IT era, business risks of an organization are closely related to web security threats facing its mission-critical services. Meanwhile, the number of web security threats grows rapidly with the number of web applications and that of vulnerabilities in these applications. A study shows[53] that on average, each website contains about 5 to 32 vulnerabilities and each revealed vulnerability has a lifecycle of 300 days, with high-risk ones even remaining active for as long as 500 days. That is to say, most websites contain vulnerabilities most of the time. Known vulnerabilities in websites, if not fixed immediately, are equivalent to business defects directly exposed on the Internet, incurring huge risks for enterprises.

Figure 7-1 Percentages of attacked sites and unattacked sites



Source: NSFOCUS MSS

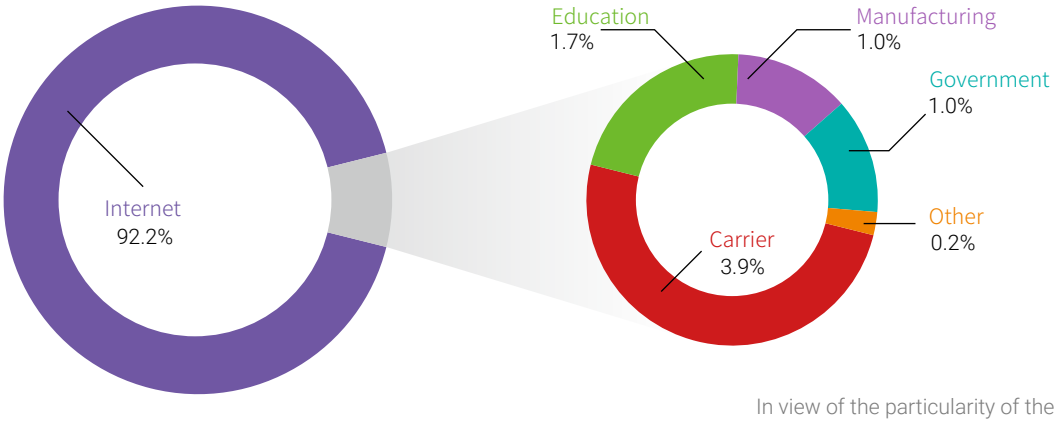
53 https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report-FINAL.pdf

7.2 Attacked Sectors

Sectors differ in business forms and infrastructure supporting business, thus suffering obviously different scales of web application attacks. In 2017, Internet enterprises, the favorite targets of web application attacks, were hit by 92.2% of this kind of attacks. Why is the Internet sector most targeted? The real reason is that a tremendous amount of business is available via web and needs the support by complex IT architectures.

In light of business characteristics, all sectors, not just the Internet sector, should pay adequate attention to web attacks. Arguably, attacks against web applications are the first step to compromising an enterprise. Such attacks, once successfully implemented, will inflict a great loss to enterprises, ranging from web page defacement and reputation damage to disclosure of large amounts of sensitive information, database deletion, and loss of vital data. What's worse is that attacked enterprises may need to undertake corresponding legal liabilities, in addition to the huge economic loss and reputational damage.

Figure 7-2 Distribution of web application attacks by sector



In view of the particularity of the financial sector, it is omitted from statistics shown in the figure.

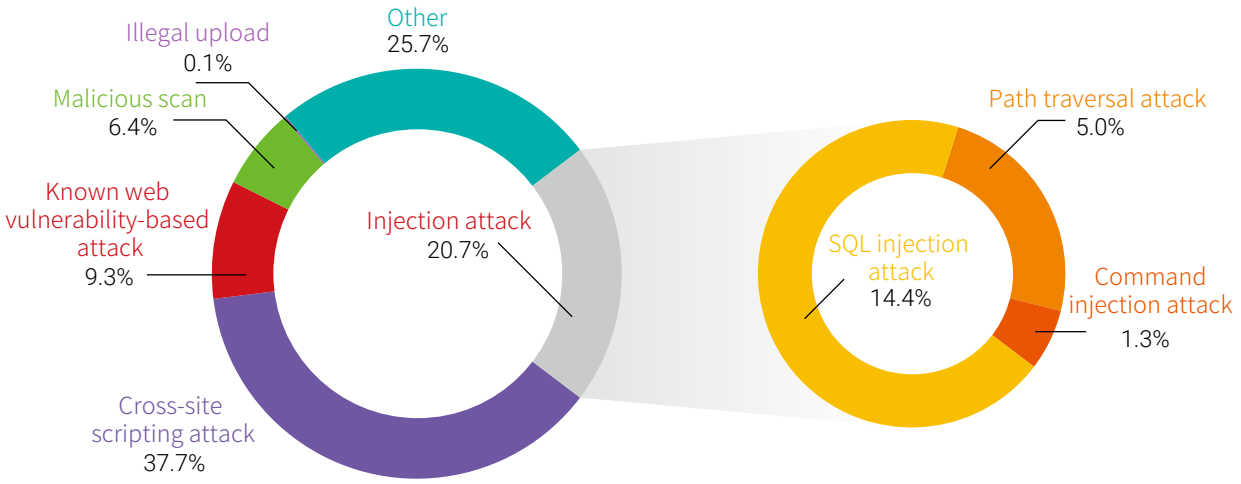
Souce: NSFOCUS MSS

7.3 Web Application Attacks

7.3.1 Attack Types

The following figure shows percentages of various web application attacks. We can see that XSS attacks rank first, taking up 37.7%. Then injection attacks come second with a percentage of 20.7%, which contain SQL injection attacks (14.4%), path traversal (5%), and command injection (1.3%) attacks. Attacks with known web vulnerabilities (including known vulnerabilities in web servers and web frameworks or plug-ins) take the third place, accounting for 9.3%. OWASP places injection attacks at the highest risk level for two consecutive years. This type of risks is graded at A1 in the OWASP Top 10 refactored in 2017.Although XSS has been downgraded from A3 to A7 in terms of risks, it is still most frequently exploited by hackers for web attacks.

Figure 7-3 Percentages of different types of web application attacks

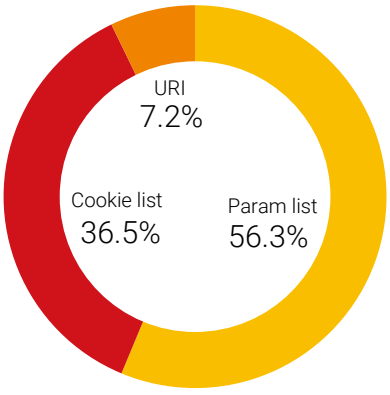


Source: NSFOCUS MSS

7.3.2 Common Payload Injection Locations of Injection Attacks

Many web attackers meticulously craft HTTP attack packets to make them look much like legitimate ones. Then they send these packets to the target server, which, in turn, responds as maliciously intended. Ultimately, the attackers will either obtain sensitive information from the system or server or upload malicious files. Here SQL injection and command injection attacks are used as an example. The following figure shows the most common locations where payloads were injected for these attacks. Obviously, the parameter list in URLs was most favored by hackers, accounting for 47.3% of the total injections or changes. Cookies come in second, accounting for 45.1%, followed by URIs.

Figure 7-4 Common payload injection locations of injection attacks



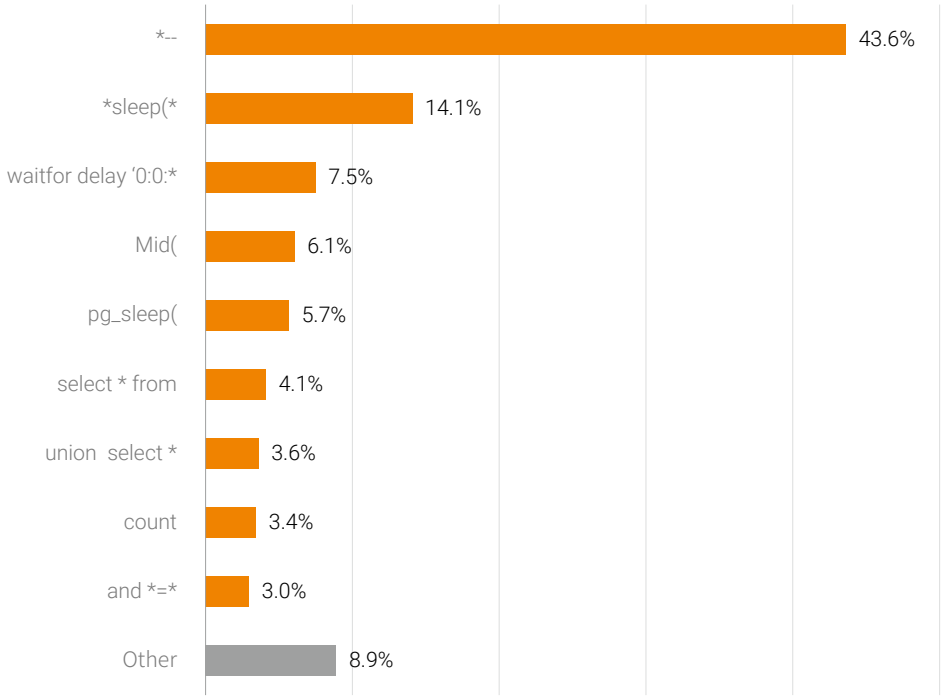
Source: NSFOCUS MSS

7.3.3 Common Payloads in SQL Injection Attacks

Among injection attacks, SQL injection attacks are commonly seen. SQL injection refers to the act of inserting SQL commands, via a normal port, to web forms to submit or entering the domain name or page request query

string, ultimately inducing the server to execute malicious SQL commands. It seems that this malicious attempt has no difference from normal access to web pages. No wonder most firewalls on the market cannot identify SQL injection and only professional web application firewalls can block such attacks with special protection methods. The following figure shows top 10 payloads injected for SQL injection attacks in 2017.

Figure 7-5 Top 10 payloads most frequently used by SQL injection attacks in 2017



Souce: NSFOCUS MSS

1. The *-- INSERT statement is most frequently used, making up 43.6% of all attack payloads. Inserting -- into an SQL statement could comment out filtering conditions, thus obtaining the data structure of the database. This simple insertion method is usually used during the early stage of database exploration.
2. The *sleep(* INSERT statement takes the second place, with a proportion of 14.1%. Similar to pg_sleep(* such as select sleep(2)-- and select pg_sleep(5)-- which are mainly used for time-based blind injection against MySQL and PostgreSQL, waitfor delay'0:0:* is usually used for time-based blind injection against the MSSQL database. Also, the return value of the sleep function is always 0 (sleep(n)=0), which could be used for SQL injection.
3. The Mid(function, with a share of 6.1%, is mainly used to truncate strings. For example, MID(DATABASE(),1,1)>'a' is used to check the first bit of the database name and MID(DATABASE(),2,1) is used to check the second bit of the database name, and so on. Such functions are usually used to guess database names and user names.

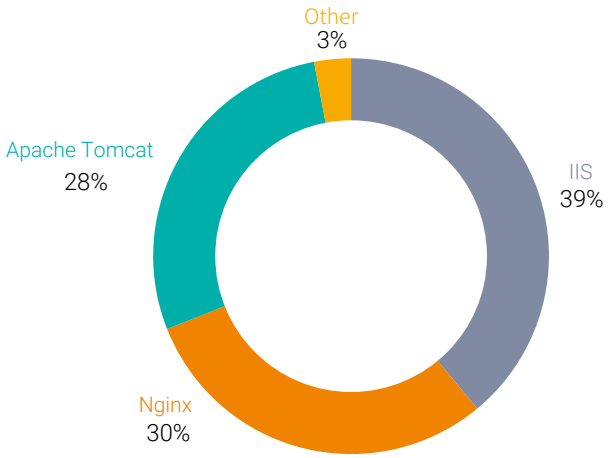
Judging from signatures included in payloads used for SQL injection attacks, we can see that most of these attacks are launched to check the existence of website vulnerabilities during the hacking process.

7.4 Attacks Exploiting Known Vulnerabilities in Web Servers

7.4.1 Types of Attacked Servers

As shown in the following figure, Microsoft IIS (39%), Nginx (30%), and Apache Tomcat (28%) are most favored targets among web servers that contain known vulnerabilities. Also, the three types of servers are most widely used to power enterprise websites.

Figure 7-6 Proportions of web server types attacked

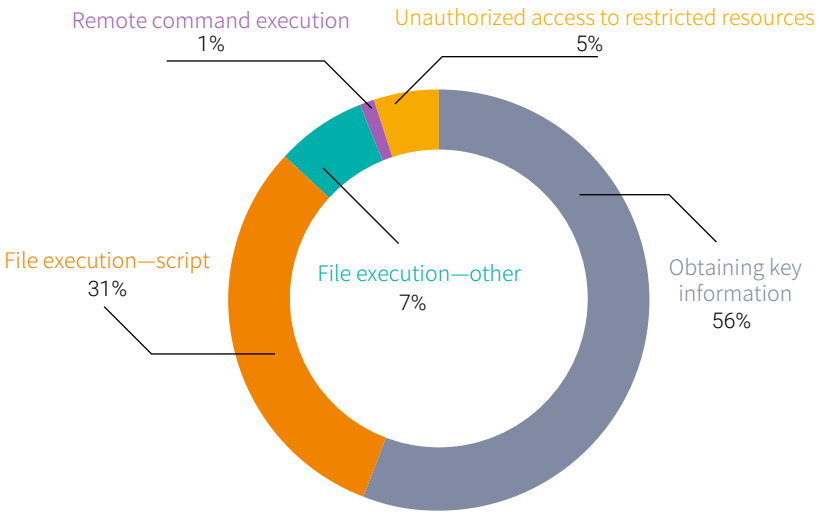


Souce: NSFOCUS MSS

7.4.2 Types of Known Vulnerabilities Exploited for Attacks

Vulnerability exploitation can, in most times, lead to disclosure of critical information, including directory and file enumeration, file path disclosure, disclosure of source code of website scripts, and read of system configuration files. This type of attacks accounts for 56% of all web attacks. Another significant type of attacks is file execution. Specifically, attackers exploit flaws in server programs' resolution of URLs and file names and leverage the file upload function to execute the uploaded files as scripts for the purpose of further intrusion via webshells. Besides, some attacks can allow access to restricted resources with escalated privileges so that attackers can read, download, and upload files at the location of a restricted directory, or even directly run executable files in the said directory.

Figure 7-7 Types of vulnerabilities in web servers exploited for attacks



7.4.3 Top 10 Vulnerabilities

The following table list top 10 vulnerabilities that are most frequently exploited in attacks against web servers in 2017. It is worth noting that this trend is consistent with that mentioned in the 2017 Midyear Cybersecurity Insights. We can see that hackers, when attacking web servers, most frequently exploit very "ancient" vulnerabilities.

Table 7-1 Top 10 vulnerabilities in web servers

Vulnerability Name	Product	Release Time	CVSS Score	Percentage of Related Attacks
Apache Tomcat mod_jk information disclosure vulnerability (CVE-2008-5519)	Apache Tomcat	2009	2.6	9.8%
Tomcat directory traversal vulnerability (CVE-2008-2938)	Apache Tomcat	2008	4.3	1.0%
IIS file upload vulnerability (CVE-2009-4445)	Microsoft	2009	6	0.5%
Microsoft IIS security extension input validation vulnerability (CVE-2010-1899)	Microsoft	2009	4.9	0.4%
nginx file traversal vulnerability (CVE-2009-3898)	Ngnix	2009	4.9	0.4%
Microsoft IIS executable file parsing vulnerability (CVE-2000-0886)	Microsoft	2000	7.5	0.3%
Apache HTTPd Range header denial-of-service vulnerability (CVE-2011-3192)	Apache Tomcat	2011	7.8	0.2%
IIS file name extension parsing error leading to ASP code disclosure (CVE-1999-0253)	Microsoft	1999	7.5	0.2%
IIS Unicode character decoding error leading to remote command execution (CVE-2000-0884)	Microsoft	2000	7.5	0.1%
IIS script file name parsing vulnerability (CVE-2009-4444)	Microsoft	2009	6	0.1%

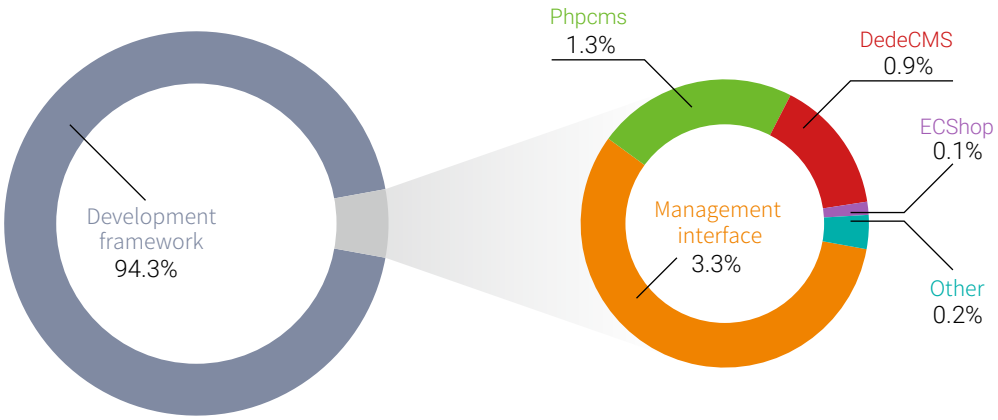
Source: NSFOCUS MSS

7.5 Attacks Exploiting Known Vulnerabilities in Web Frameworks and Applications

7.5.1 Attacked Web Frameworks or Applications

A web framework is a software framework that is designed to support the development of web applications, including dynamic websites, web application programs, and web services. Many universal web service systems are also developed based on similar frameworks. Examples of web frameworks are Django, ThinkPHP, Apache Struts, and Spring. Web applications include various content management systems (DedeCMS, ECShop, WordPress, phpBB, phpCMS, and PHPWind) built with PHP, JSP, and ASP, as well as web applications that are used for UI management. In 2017, attacks targeting framework programs are most frequently seen, accounting for 94.3% of the total attacks. Struts 2 is a typical example that attracts much attention from attackers.

Figure 7-8 Attacked web frameworks or applications



7.5.2 Top 10 Vulnerabilities

The following table shows top 10 known vulnerabilities that are most frequently used to attack web frameworks or applications. Obviously, vulnerabilities in Apache Struts 2 are most favored by attackers, taking seven (including two revealed in 2017) spots in this list. On March 7, 2017, a critical vulnerability (CVSS score: 10) was reported in Apache Struts 2 and then assigned CVE-2017-5638. Exploitations associated with this vulnerability accounted for 16.8% of the total with known vulnerabilities. For details of the impact, exploitation, and remediation of this vulnerability, see the NSFOCUS's *2017 H1 DDoS and Web Application Attack Landscape*. For details about the Apache Struts 2 REST plug-in vulnerability (CVE-2017-9805) revealed in September 2017, see section 7.9.1 Apache Struts 2 REST Plug-in Vulnerability (CVE-2017-9805).

Table 7-2 Top 10 vulnerabilities in web frameworks or applications

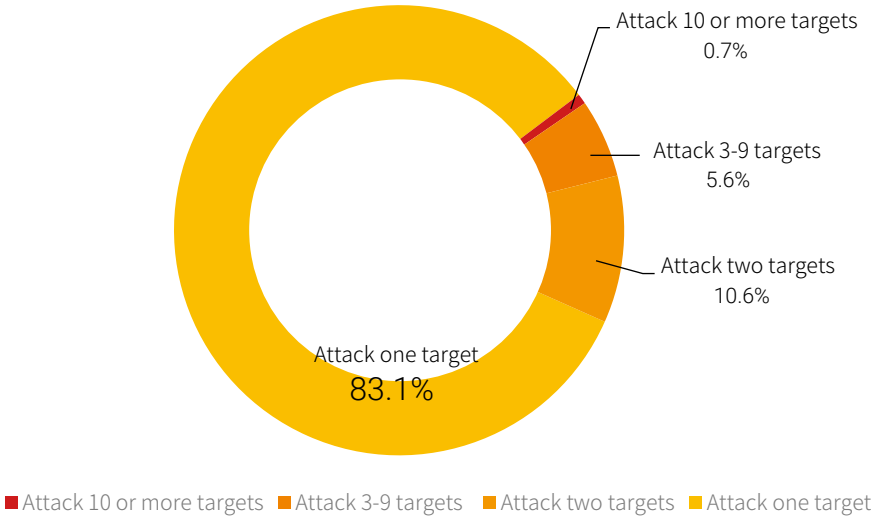
Vulnerability Name	Product	Release Time	CVSS Score	Percentage of Related Attacks
Apache Struts 2 REST plug-in remote code execution vulnerability (CVE-2016-4438)	Apache Struts2	2016	7.5	49.8%
Apache Struts 2 Jakata plug-in remote code execution vulnerability (CVE-2017-5638)	Apache Struts2	2017	10	16.8%
Apache Struts 2 REST plug-in vulnerability (CVE-2017-9805)	Apache Struts2	2017	6.8	7.6%
Apache Struts 2 Remote Code Execution Vulnerability (CVE-2013-1966)	Apache Struts2	2013	9.3	6.9%
Apache Struts 2 Remote Code Execution Vulnerability (CVE-2013-2251)	Apache Struts2	2013	9.3	4.8%
Elasticsearch sandbox bypass remote code execution vulnerability (CVE-2015-1427)	ElasticSearch	2015	7.5	0.4%
Apache Struts 2 ClassLoader manipulation vulnerability (CVE-2014-0094)	Apache Struts2	2014	5	0.3%
Apache Struts 2 malicious Ognl expression remote code execution vulnerability (CVE-2016-3081)	Apache Struts2	1916	9.3	0.2%
DedeCMS multiple SQL injection vulnerabilities (CVE-2011-5200)	DedeCMS	2012	7.5	0.1%
Pivotal Spring Data REST, Spring Boot, and Spring Data vulnerability (CVE-2017-8046)	pivotal_software	2017	7.5	0.1%

Source: NSFOCUS MSS

7.6 Target Scope and Reputation of Source IP Addresses of Web Attacks

Analyzing the scope of source IP addresses of web attacks, we find that 16.9% of IP addresses targeted two or more websites.

Figure 7-9 Percentages of source IP addresses attacking varying numbers of targets



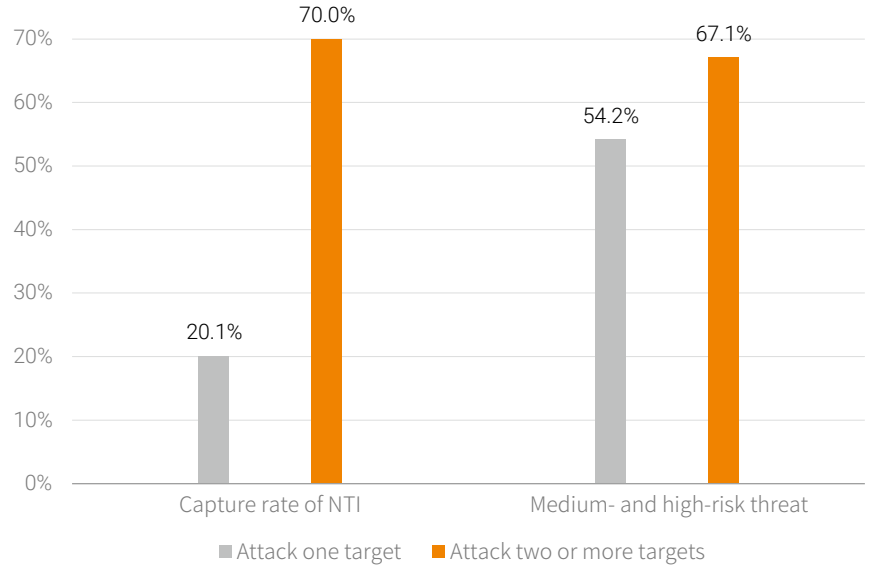
Source: NSFOCUS NTI

Consulting NTI for reputation of these IP addresses, we discovered that, among all source IP addresses attacking one website, 54.2% had bad reputation records and were marked as medium-risk or high-risk; among those attacking multiple (2 or more) websites, 67.1% were marked as medium-risk or high-risk. This indicates that the more targets an IP address attacks, the more active this IP address is and the more probable it is marked as abnormal and high-risk on NTI.

This reputation data differs from that of DDoS attack sources (see section 5.2.4) in such aspects as the capture rate and probability of being marked as high- or medium-risk. For example, as for attack sources (hitting two or more targets) that are regarded as "recidivists", the capture rate is 94.1% for DDoS attacks and 70% for web attacks and the probability of being marked high- or medium-risk is respectively 20.9% and 67.1%. The reason is that as attacks differ in attack nature, attack means, and impact, NTI handles sources of different kinds of attacks in different ways. For example, an ongoing DDoS attack may render the target service unavailable by consuming network bandwidth or service resources. However, once the attack ends, the target service will become available again. In contrast, web application attacks, with a high degree of concealment, are launched to obtain system privileges and confidential data in most cases. Once successfully implemented, this kind of attack will have a longer-term impact (direct impact on business, instead of indirect impact such as reputation damage or loss of business) on targets. Besides, web attack sources often have real IP addresses. To achieve the malicious purpose, the attacker tends to carry out an attack step by step, for example, first scan the website for vulnerabilities and then drop the exploit for penetration. Once compromising a system, the attacker may take control of it and perform malicious operations such as stealing confidential data and corrupting the database. Therefore, it is understandable why source IP addresses of certain types of web attacks are assigned a higher threat level.

In 2017, we made a source IP address comparison between DDoS and web attacks and found that nearly 50,000 attack sources were involved in both types of attacks. Among such attack sources, 60% performed scanning activities, of which 88.3% were marked high- or medium-risk. Despite the fact that they may not belong to any hacking group, these IP addresses are more possible to be controlled by hackers and become their "fixed assets" than others due to the loose control of hosting providers and host owners on their own assets. These IP addresses, though only a small proportion, cause much trouble and confusion. According to the *2017 Annual Cybersecurity Insights* released by NSFOCUS, 0.39% of attack sources in the network are responsible for 90% of attack events.

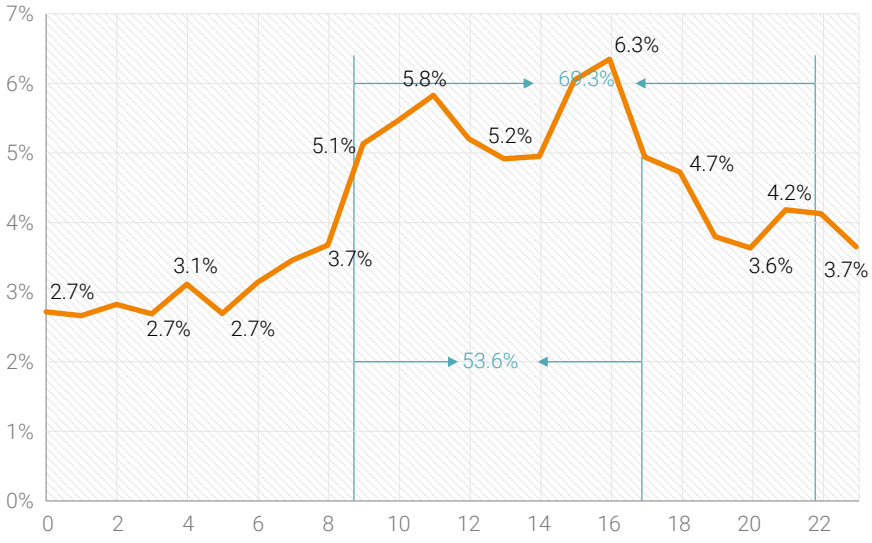
Figure 7-10 Proportions of source IP addresses with different capture rates and risk levels



7.7 Time Distribution of Web Application Attacks

The following figure shows the distribution of web application attacks in 24 hours. The peak hours for web business are 9:00 to 22:00, during which web application attacks occur frequently. Web business surges, in particular, from 9:00 to 17:00, when attackers are most active, implementing 53.6% of all web attacks.

Figure 7-11 Overall distribution of web application attacks in 24 hours

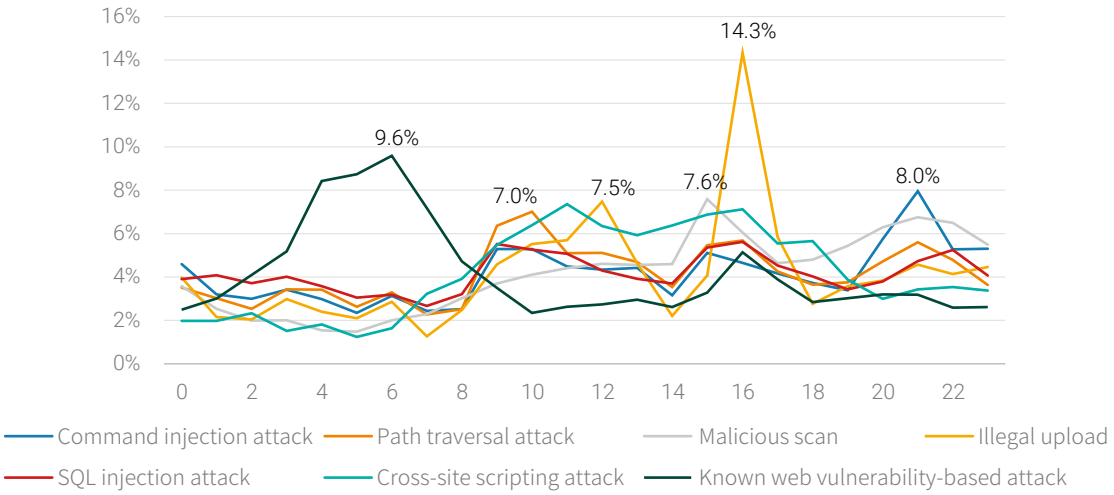


Source: NSFOCUS MSS

The following figure shows the distribution of various web attacks in 24 hours. We can see that the early morning saw a portion of web attacks exploiting known vulnerabilities which reached the peak from 4:00 to 6:00. With the aid of automated tools, most of those attacks need no interaction with clients. Other types of vulnerabilities,

however, usually surged during peak hours (9:00 to 22:00) of web business, causing more serious impact and damage.

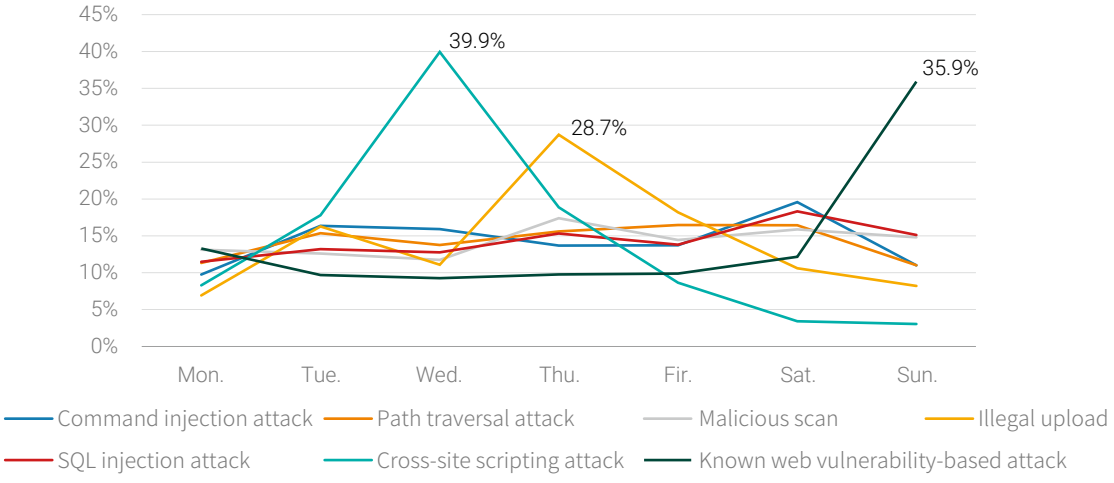
Figure 7-12 Distribution of various web application attacks in 24 hours



Source: NSFOCUS MSS

The following figure shows the trend of eight types of web attacks in a week. Wide fluctuations are observed in cross-site scripting attacks, illegal upload, and web attacks exploiting known vulnerabilities. XSS attacks experienced a big jump on Wednesday (39.9% of the week's total such attacks), but a sharp decrease on Saturday and Sunday (3%). The second peak came on Thursday because of Illegal uploads (28.7% of the week's total such attacks). For web attacks exploiting known vulnerabilities, there were not so many on weekdays, but a sharp increase on Sunday (35.9% of the week's total such attacks). This had much to do with the use of automated means. Other types of attacks were relatively evenly distributed throughout the seven days.

Figure 7-13 Distribution of various web application attacks in a week



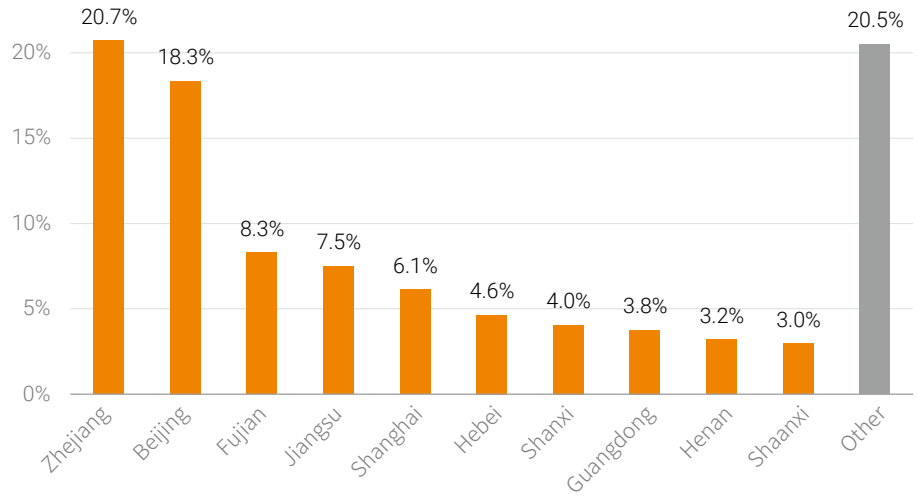
Source: NSFOCUS MSS

7.8 Geographical Distribution of Web Application Attacks

7.8.1 Geographical Distribution of Attack Source Hosts

The following figure shows the distribution of web application attack sources in China, with Zhejiang province (20.7%) and Beijing (18.3%) taking the top two spots.

Figure 7-14 Distribution of web application attack sources in China

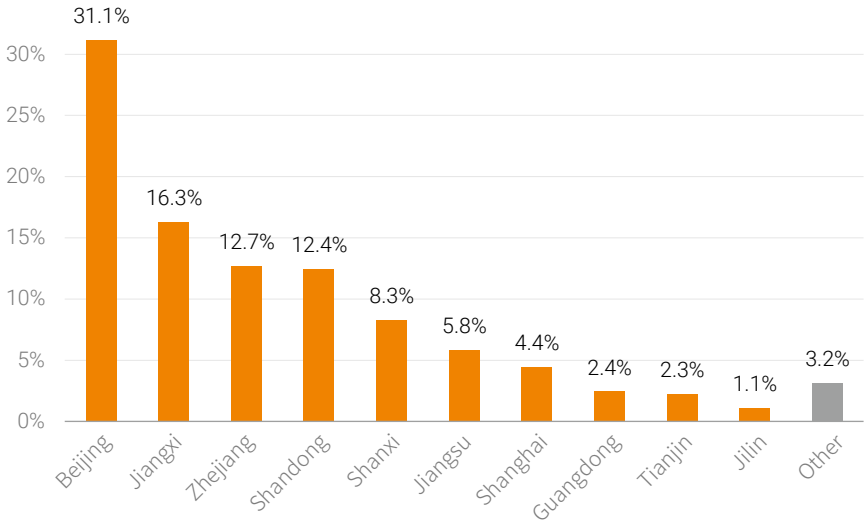


Source: NSFOCUS MSS

7.8.2 Geographical Distribution of Attack Targets

The following figure shows the distribution of web application attack targets in China. We can see that Beijing ranks first with a proportion of 31.1% and Jianxi province comes second, taking up 16.3% of the total.

Figure 7-15 Distribution of web application attack targets in China



Source: NSFOCUS MSS

7.9 Topical Vulnerabilities

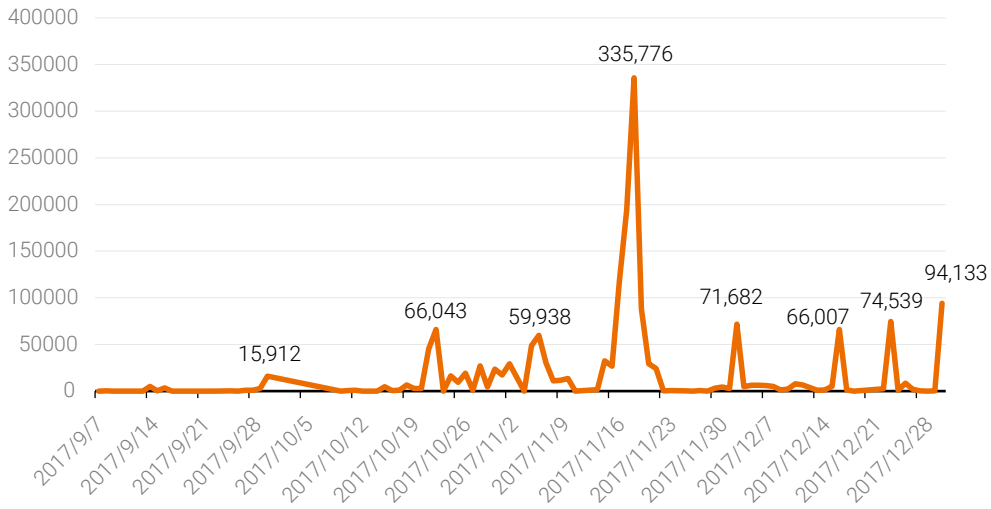
7.9.1 Apache Struts 2 REST Plug-in Vulnerability (CVE-2017-9805)

In September 2017, a vulnerability[54] (CVSS score: 6.8) was reported in Apache Struts 2 and then assigned CVE-2017-9805. This vulnerability exists in the REST plug-in in Apache Struts 2.5 through 2.5.12 and 2.1.2 through 2.3.33. The REST plug-in in Apache Struts 2 uses an XStreamHandler with an instance of XStream for deserialization of XML payloads, without any kind of filtering. A remote attacker, via maliciously crafted XML content, could exploit this vulnerability to obtain business data or server privileges, finally causing arbitrary code execution.

As one of the most popular Java web server frameworks around the world, Apache Struts 2 is widely used for the underlying template building of portal websites of governments, enterprises, and the financial sector. However, this framework contains many vulnerabilities, with eight (including four high-risk ones) exposed in 2017 alone. As shown in Figure 6-10, among web framework or application programs, Apache Struts 2 is the most popular in terms of vulnerability exploitation, taking seven places on the list of top 10 vulnerabilities.

The following figure shows the attack trend from September 7, 2017 to December 31, 2017. During the three months, NSFOCUS detected 1,712,983 attacks against all websites under its monitoring, discovering a sharp increase from November 16 to 21, with the daily peak reaching 335,776.

Figure 7-16 Trend of attacks exploiting the vulnerability (CVE-2017-9805) from September 7 to December 31



Source: NSFOCUS MSS

We advise enterprises to fix this vulnerability immediately and deploy related detection and protection measures. Also, NSFOCUS issued the *Struts 2 s2-052 REST Plug-in Remote Code Execution Technical Analysis and Solution*[55], presenting a vulnerability handling method and remediation solution as well as a vulnerability detection

54 http://blog.nsfocus.net/struts2-s2-052-rest-plug-in-remote-code-execution-technical-analysis/
55 http://blog.nsfocus.net/struts2-s2-052-rest-plug-in-remote-code-execution-technical-analysis/

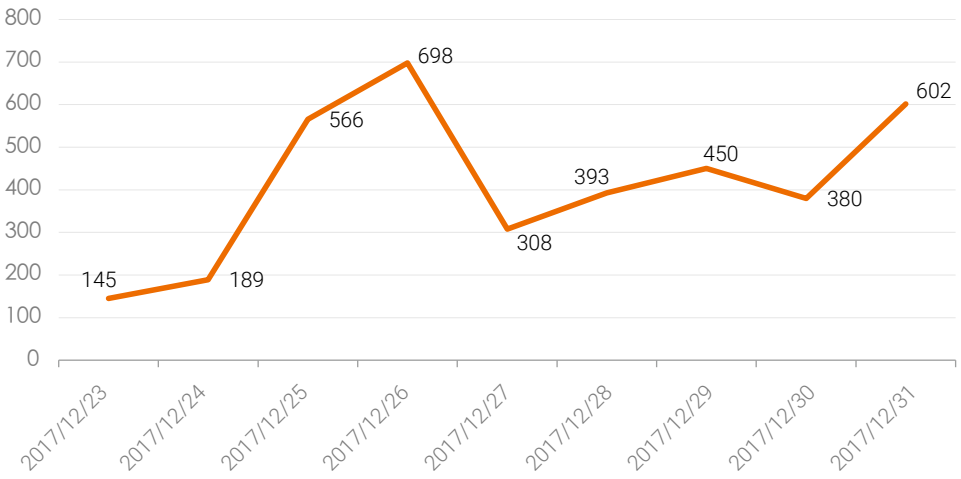
and protection method implemented with security devices such as WAF, NF, IPS, RSAS, and WVSS.

7.9.2 WebLogic XMLDecoder Deserialization Vulnerability (CVE-2017-10271)

On October 23, 2017, a vulnerability (CVSS score: 7.5) in the Oracle WebLogic Server component in Oracle Fusion Middleware was revealed and assigned CVE-2017-10271[56]. Oracle Fusion Middleware is a business innovation platform developed by the US corporation Oracle for enterprises and clouds. This platform provides middleware and software integration functions, in which Oracle WebLogic Server is an application server component used for clouds and traditional environments. A vulnerability exists in the WLS Security subcomponent in the Oracle WebLogic Server component in Oracle Fusion Middleware. Via an HTTP request that contains a crafted XML payload, an attacker could exploit this vulnerability to gain privileges of the targeted server, causing arbitrary code execution. Also, this vulnerability allows an attacker to control the Oracle WebLogic Server, thus compromising the data availability, confidentiality, and integrity.

The following figure shows the trend of vulnerability-based attacks against websites under our monitoring in the last nine days (December 23 to 31) of 2017. A total of 3397 attacks were detected during the period, with the daily peak of 698 on December 26.

Figure 7-17 Trend of attacks exploiting the vulnerability (CVE-2017-10271) from December 23 to 31



Source: NSFOCUS MSS

Shortly after the vulnerability (CVE-2017-10271) in the WebLogic WLS component was reported, NSFOCUS received a slew of security reports from customers of different sectors. Analyzing these reports, we found that attackers exploited this vulnerability to plant the cryptocurrency miner watch-smartd[57] in WebLogic hosts, making it run on the hosts to consume considerable CPU and memory resources of servers. Besides, this miner, once successfully infecting a target, is difficult to remove.

Though this vulnerability (CVE-2017-10271) is actively exploited in the wild, no details about it are disclosed.

56 http://toutiao.secjia.com/nsfocus-internet-security-threats-weekly-201750
57 http://toutiao.secjia.com/weblogic-host-mining

Official patches were released in October 2017, but a great number of enterprises failed to install them in time. Currently, this vulnerability is mainly used to propagate miners, but we cannot rule out the possibility that hackers may exploit it for other malicious purposes, including building a botnet for DDoS attacks. An attacker exploiting this vulnerability can target both Windows hosts and Linux hosts at the same time and hide in them in an unnoticeable manner for a long period. As Oracle WebLogic is widely used, attacks exploiting this vulnerability will definitely spread across various sectors. In view of this, we recommend that enterprises immediately patch vulnerable hosts, update the related vulnerability check and protection plug-in in security protection devices, as well as adjust protection policies accordingly.

The *WebLogic WLS Component Vulnerability Handling Suggestions*[58] and *WebLogic WLS Component Vulnerability Technical Analysis and Solution*[59] issued by NSFOCUS provides a vulnerability handling method and remediation solution as well as a vulnerability detection and protection method implemented with security devices such as WAF, NF, IPS, RSAS, and WVSS.

58 http://blog.nsfocus.net/weblogic-solution/
59 http://blog.nsfocus.net/weblogic-vulnerability/

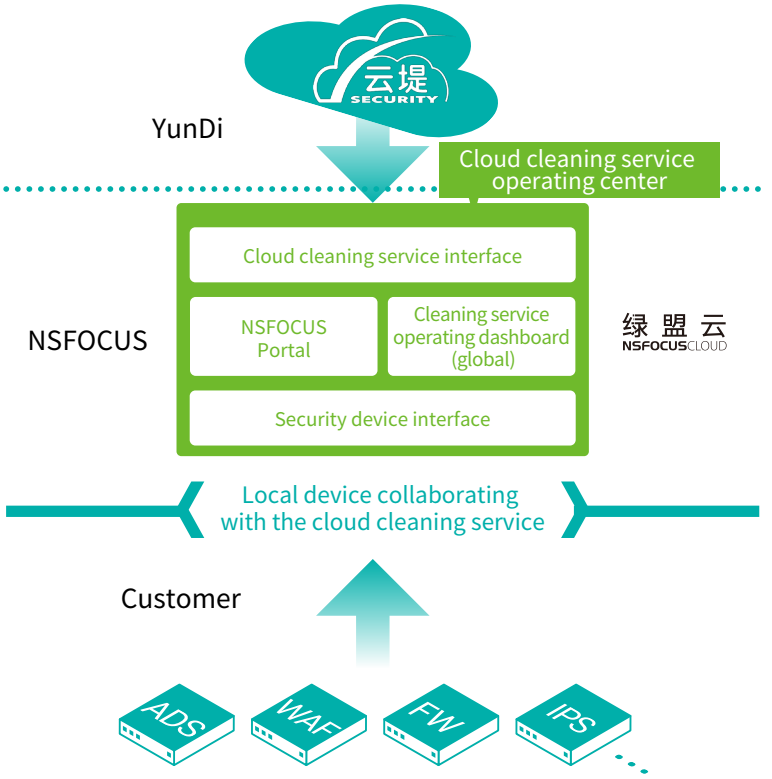
8. Protection Against DDoS and Web Application Attacks

Under the background of “cloud”, “big data”, “IoT”, and “mobilization”, cyber security threats are constantly changing and traditional defense methods are challenged.

8.1 DDoS Protection

DDoS attacks are growing in size. In 2017, we find that there is about a threefold increase in super large attacks over 300 Gbps and attacks with more than 100 Gbps traffic have been a normal trend. Besides, new attack techniques and means never cease to emerge. IoT botnets are upgrading rapidly, reducing a lot of IoTs to attack tools. Also, DDoS attack services are more easily available and increasingly industrialized, keeping the cost for launching DDoS attacks down. Thus, it can be very challenging to counter this type of attacks. Generally, protective hardware devices are deployed on premises so that traffic can be cleaned as close to the destination as possible and protection policies can be adjusted according to the actual business of customers. However, such a protection solution fails to resist high-volume attacks due to the limited access bandwidth resources. Many customers are faced with such an issue: Due to the lack of IT security professionals, they are unable to promptly respond to or defend against DDoS attacks that cause bandwidth saturation. To solve this issue, major carriers and vendors start to provide cloud cleaning services such as YunDi from China Telecom. YunDi provides a groundbreaking near-source cleaning service that solves the bandwidth consumption issue by utilizing resources throughout the network of China Telecom for traffic cleaning near the attack source. By collaborating with China Telecom to leverage advantages of YunDi, NSFOCUS provides the innovative hybrid cleaning technique that combines on-premises security devices and the cloud, delivering ideal protection and cleansing results.

Figure 8-1 Cloud cleaning scenario



The following is the cleaning scenario of our hybrid cloud:

1. A customer has deployed NSFOCUS's security devices and purchased NSFOCUS's cloud cleaning service.
2. After the cloud cleansing service is successfully subscribed, the customer will get a self-service account from NSFOCUS, and then complete cloud collaboration configurations on on-premises devices. After that, on-premises devices will upload the identified DDoS attack traffic information to NSFOCUS cloud. If the attack traffic at the customer end exceeds a specified threshold, an on-premises security device will automatically collaborate with the NSFOCUS cloud for cleaning. Alternatively, the device may send an SMS notification to the administrator who will decide whether collaboration with the cloud is required and, if it is, will then manually start it with a click of the related button on the UI.
3. The administrator can view real-time traffic cleaning information (reports on cloud cleaning and local cleaning) on the self-service page. NSFOCUS O&M engineers keep a close eye on the customer' DDoS cleaning status on the O&M interface.

Cloud cleaning can thwart volumetric attacks to prevent bandwidth exhaustion. However, this solution requires more bandwidths that are quite costly and can hardly deliver precision protection based on characteristics of customer business. As such, customers tend to hesitate at choosing this solution. In response to this issue, NSFOCUS provides customers with a hybrid cleaning solution that integrates the cloud and on-premises anti-DDoS devices, with low- and medium-scale attacks dealt with by on-premises devices and volumetric attacks handled remotely by the cloud with which the devices collaborate.

Figure 8-2 Hybrid protection solution

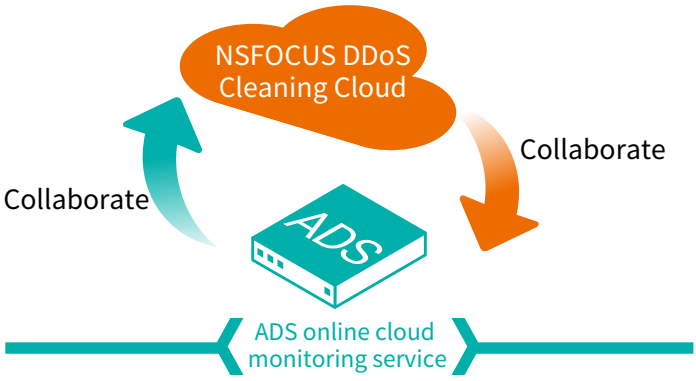
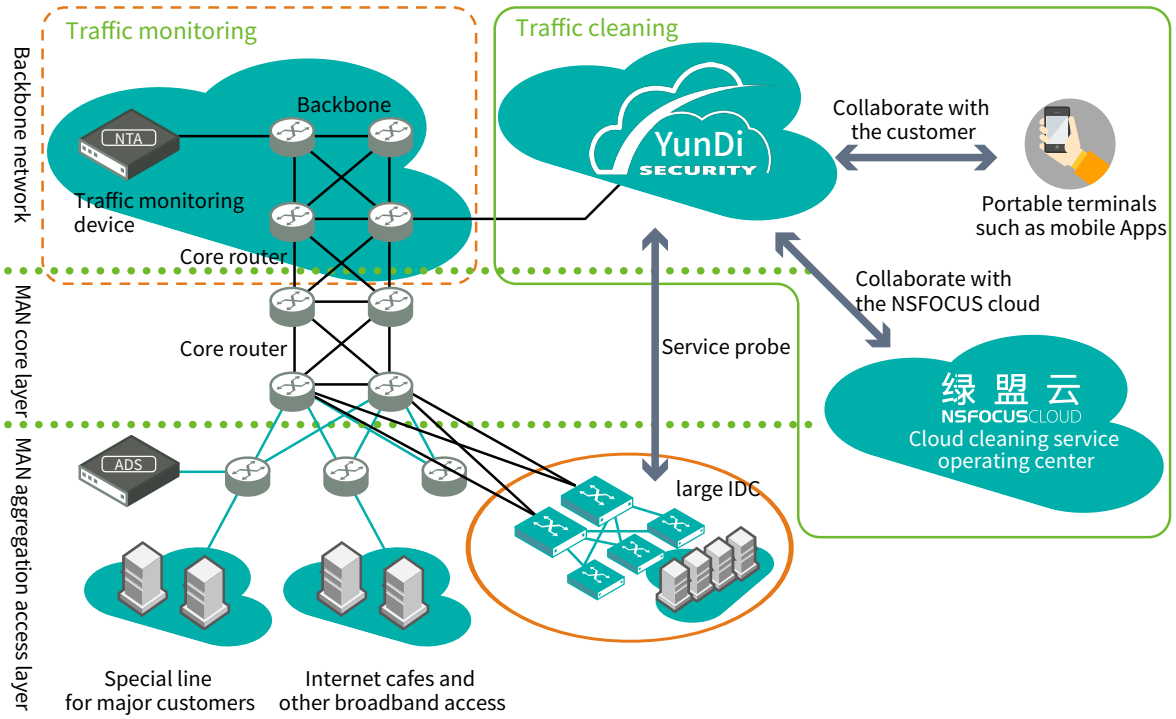


Figure 8-3 Deployment of the hybrid protection solution



The hybrid DDoS cleaning solution has the following merits:

1. Rapid attack response
2. High defense capability
3. Business confidentiality ensured: Most attacks are handled by on-premises protective devices and only volumetric attacks are diverted to the cloud.
4. Cost-effective: Customers do not need to invest a lot in creation of such a hybrid protection system.
5. Sufficient defense bandwidth: DDoS attacks over 300 Gbps can be blocked.

Based on a decade's experience in DDoS prevention and continuous product innovation, NSFOCUS launched ADS NX5-10000 with a throughput of 240 Gbps in 2017, meeting the high-performance DDoS cleaning requirement of backbone networks and metropolitan area networks (MANs) of carriers, large data centers, and cleaning centers. In combination with global botnet intelligence and IP reputation provided by NSFOCUS NTI and NSFOCUS ATM's attack alerts based on big data analysis, ADS NX5-10000 delivers prompt smart DDoS protection, thus ensuring continuous, secure, and stable business operations of customers.

8.2 Web Application Attack Protection

Our web application attack trend analysis (see chapter 7) suggests that XSS, injection attacks, and malicious scans remain web attack vectors that are most frequently used by hackers. Third-party components integrated in websites are more prone to security issues, while known vulnerabilities are still hackers' main point of entry to the websites. Vulnerability information and exploits are spread so rapidly via social media and other channels that it has become increasingly easier to test attacks. The prevalence of automated attacks, typically scans, leading to more website vulnerabilities exposed, thus facilitating hacker intrusions.

Our investigation on customers' business reveals that as virtualization and cloud platforms gain popularity, more and more customers migrate their public web services to clouds, thus placing a greater demand on cloud-based web security protection. This corroborates a strategic planning assumption of Gartner that by the end of 2010, over 50% of public web services will be protected by cloud-based WAF service platforms which integrates content delivery networks (CDNs), DDoS protection, botnet mitigation, and WAF.

In view of the current market trend and web application attacks discovered in 2017, we come to two conclusions:

- Web application attack protection must incorporate both detection and response, instead of relying solely on defense.
- Rather than emphasizing node-by-node detection and merely alerting, we should provide all-around web security protection by combining resources from multiple parties and service operations. NSFOCUS's web application protection solution can effectively mitigate top 10 risks classified by the Open Web Application Security Project (OWASP) and block threats of automated attacks, ensuring website availability. This solution involves the following products and services:

1. Cloud security

Adapting to various public cloud platforms such as Alibaba Cloud, Amazon Web Services (AWS), Microsoft Azure, Tencent Cloud, and Huawei Cloud, NSFOCUS WAF provides cloud security protection for customers' websites deployed in those clouds, delivering value-added security services for cloud platform vendors.

2.Threat intelligence

The automated attack protection solution supports device collaboration. Collaborating with NSFOCUS NTI, NSFOCUS WAF can obtain the latest reputation data of high-risk IP addresses and automatically generate related protection policies. With the IP reputation library, NSFOCUS WAF can effectively block hackers with credential stuffing attacks and econnoisseurs (click farm) and reduce false positives concerning suspicious attack behaviors to increase alert accuracy.

3. Multi-engine protection system

A better smart detection engine, based on machine learning, is introduced to learn massive samples and build normal traffic models for attack detection, thus reducing false positives and false negatives. Arguably, such engine is a useful supplement to traditional protection rules.

With flexible and fine-granularity rules and algorithms, a core protection engine supports flexible detection objection definitions, logical combinations of multiple detection conditions, as well as custom rules that can describe complex scenarios in the way natural languages do. In this manner, this engine implements effective and precise protection.

A smart patch engine is provided. That is to say, NSFOCUS WAF can collaborate with NSFOCUS WVSS to form a closed-loop process of detection and protection. During the collaboration, NSFOCUS WVSS generates detection reports and NSFOCUS WAF generates protection policies to provide hour-level security assurance and continually improve website security.

The auto-learning engine adopts the mechanism of auto-learning plus whitelist to greatly improve 0-day protection and targeted protection. With the automatic learning technique based on statistical methods, this engine analyzes user behaviors and HTTP request parameters of specified URLs, thereby assisting the administrator in building models of normal business traffic and developing whitelist rules.

4. Collaboration with ADS for DDoS protection

NSFOCUS WAF can collaborate with NSFOCUS Anti-DDoS System (ADS) which will deal with volumetric DDoS attacks that saturate WAF's upstream bandwidth. This makes up for the shortage of WAF that lacks strong cleaning capabilities. Obviously, proper cleaning resource (including anti-DDoS module of NSFOCUS WAF and resources in the cleaning center) scheduling based on the attack volume is an important highlight of NSFOCUS's web security solution.

5. Support for operations

NSFOCUS WAF with Managed Security Service (MSS), a customer-oriented service, connects and synchronizes on-premises NSFOCUS WAF with the NSFOCUS cloud to provide remote IT security detection and management, thus supporting device operations and security operations.

6. Forensics

This function is introduced for post-event analysis and reproduction of attacks. It can also be used to associate a user with all his or her web behaviors, thus revealing the user's hidden motive.

Authors

YunDi of China Telecom: Zhang Min, Chang Liyuan, Liu Ziqian, Liu Changbo, Chen Lin, Tong Xinzhe

NSFOCUS: Pan Wenxin, Peng Chang, Li Kai, Chen Jun, Zhan Shengjun, He Kun

Editors

Hao Ming and Huang Zhu (graphic designer) from NSFOCUS

2017 DDoS and Web Application Attack Landscape

中国电信·云堤 CHINA TELECOM

NSFOCUS