NSFOCUS

2016 Q3 Report on DDoS Situation and Trends

(2016-10-20)

© 2016 NSFOCUS

■ Copyright © 2016 NSFOCUS Technologies, Inc. All rights reserved.

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

Contents

Figures

1 Overview

- In Q3, the global distributed denial-of-service (DDoS) attacks increased by 40%.

  In Q3, a total of 71,416 DDoS attacks were detected, up 40% from Q2 (50,988).

- The proportion of low-volume DDoS attacks increased by 10.8% and that of and high-volume DDoS attacks decreased by 6.7%.

  20–50 Gbps medium-volume DDoS attacks and 50–300 Gbps high-volume DDos attacks respectively decreased by 4.1% and 6.7% from Q2, but low-volume DDoS attacks (less than 20 Gbps) increased by 10.8%.

- Super high-volume DDoS attacks (over 300 Gbps) occurred 35 times.

  In Q3, super high-volume DDoS attacks (over 300 Gbps) occurred 35 times, up 119% from Q2 (16 times).

- The average peak traffic of individual DDoS attacks was 19.4 Gbps.

  In Q3, the average peak traffic of individual DDoS attacks was 19.4 Gbps, which was 16.7 Gbps in Q2.

- The highest peak traffic of individual DDoS attacks reached 572.6 Gbps.

  In Q3, the highest peak traffic of individual DDoS attacks reached 572.6 Gbps, 126.9 Gbps higher than that in Q2 (445.7 Gbps).

- On average, each IP address was redundant attacked 1.4 times a month.

  In Q3, each IP address was redundant attacked 1.4 times a month on average. In particular, we found a network attacked 30 times, mostly with mixed traffic of UDP flood and NTP request flood attacks that did not last long.

- The average DDoS attack duration was 7.2 hours.

  In Q3, the average DDoS attack duration was 7.2 hours, slightly decreasing from Q2 (8.1 hours). The most durable DDoS attack lasted 31 days and over 19 hours (764 hours), generating 17 TB of traffic in total.

- The proportion of multi-vector attacks increased by 6.6 percentage points.

  Multi-vector attacks accounted for 40.3% of the total attack traffic, up 6.6 percentage points from Q2. Attacks consisting of two or three traffic types took up 99.7% of multi-vector attacks. Most frequently, NTP reflection traffic was mixed with UDP traffic.

- The proportion of reflection attacks accounted for 90.5%, up 20.6 percentage points.

  Reflection attacks accounted for 90.5% of total attacks, sharply up 20.6 percentage points from Q2. NTP reflection attacks increased most significantly.

- The number of global active NTP reflectors increased by 440%.

  In Q3, the number of active reflectors involved in DDoS attacks reached 25,371 globally, up 440% from Q2.

- The number of Mirai-infected Internet of Things (IoT) devices reached 1.5 million.

  IoT devices are a new favorite for hackers' botnet. By the end of October 2016, the number of Mirai-infected devices had reached 1,508,059. Botnet attacks had been extremely active recently. Port 23 was scanned a maximum of 340,000 times in a day.

2 Attack Situation

In Q3, 71,416 DDoS attacks were detected around the world. China was attacked most frequently, seeing 39% of the attacks, followed by the USA with 23.6% of the attacks. Compared with Q1 and Q2, the number of attacks targeting China decreased by 19.9% and 14.2% respectively, but that targeting the US slightly increased.

Figure 2-1 Global DDoS attack trend in Q3

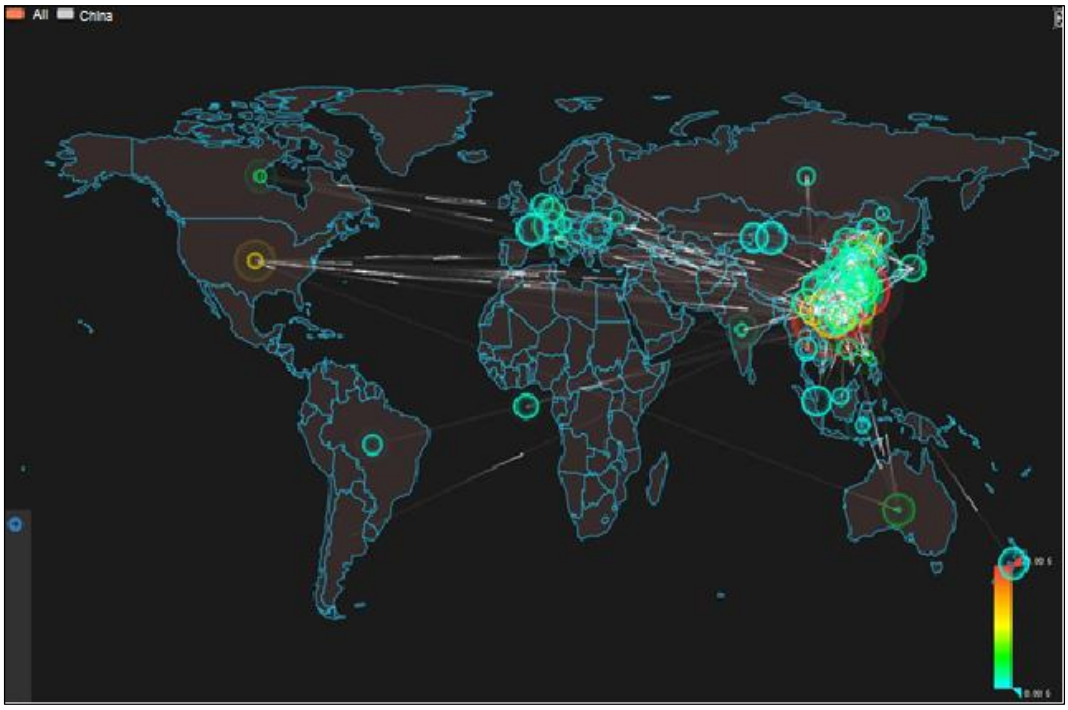


Figure 2-2 Top 10 countries under attack by the number of attacks in Q3

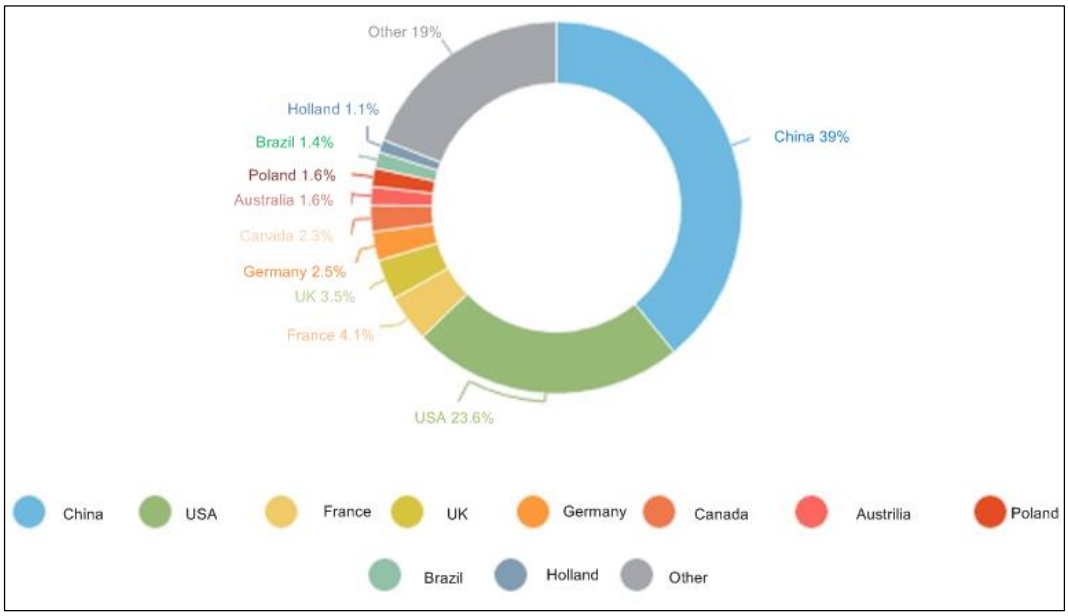
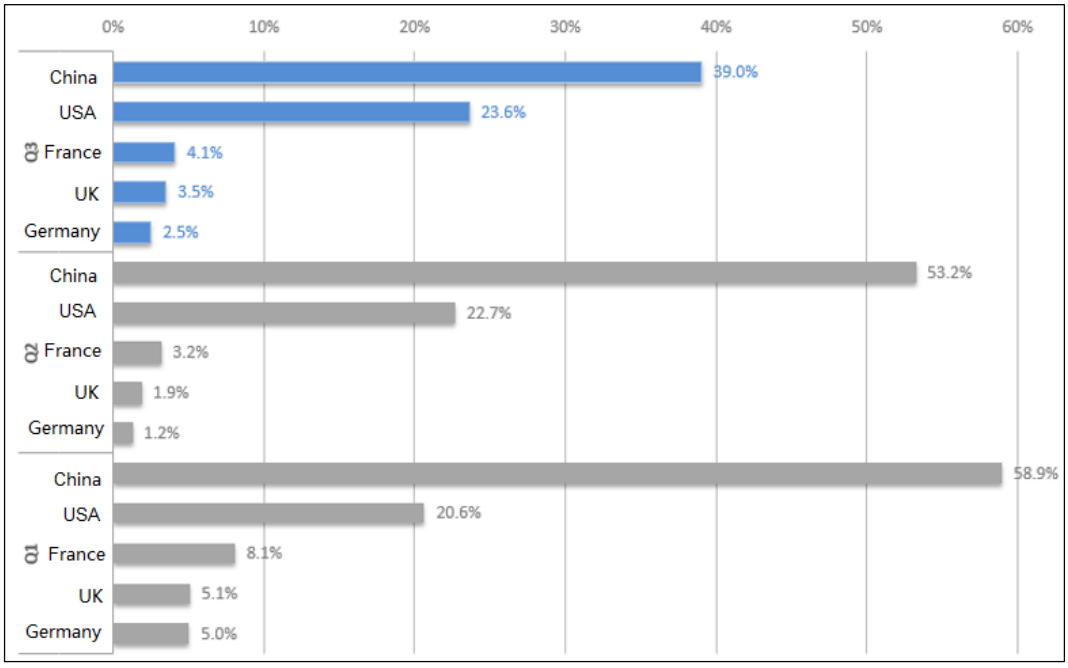
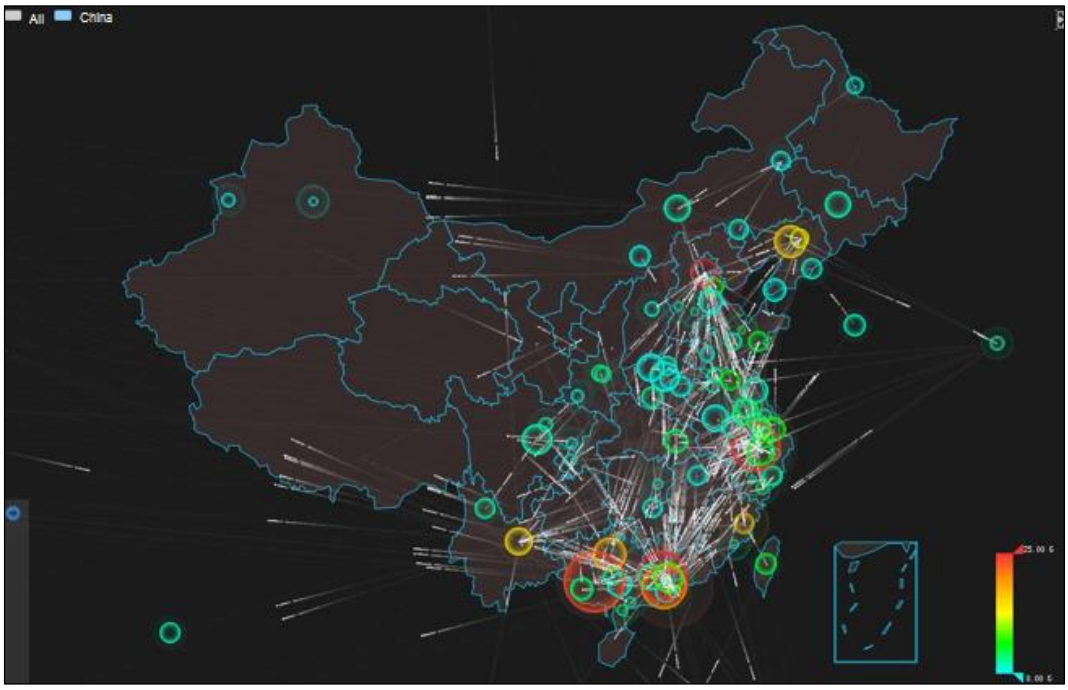


Figure 2-3 Top 5 countries under attack by the number of attacks in Q1–Q3



In Q3, 27,852 DDoS attacks were launched in China. Zhejiang, Guangxi, Guangdong, Beijing, and Jiangsu were attacked most frequently.

Figure 2-4 DDoS attack trend in China in Q3



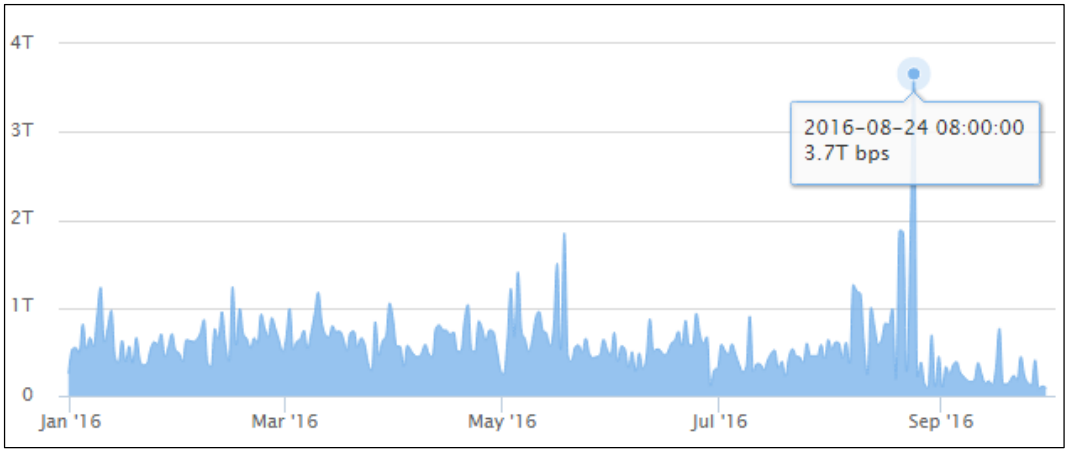
3 Attack Trends

3.1 Peak Traffic of DDoS Attacks

In Q3, the average peak traffic of individual DDoS attacks was 19.4 Gbps, up 16.2 percentage points from Q2 (16.7 Gbps) and down 31.2 percentage points from Q1 (28.2 Gbps).

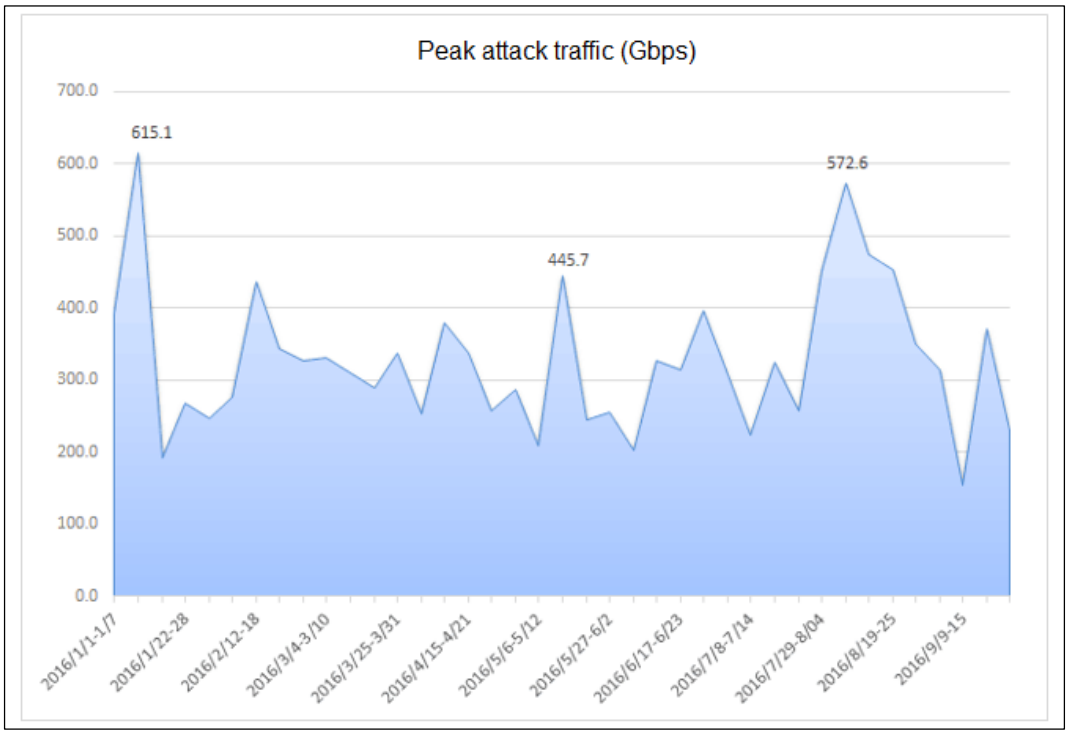
In Q3, the aggregate attack traffic peaked at 3.7 Tbps, increasing by 1.9 Tbps from Q2 (1.8 Tbps) and 2.5 Tbps from Q1 (1.2 Tbps).

Figure 3-1 Global trend of aggregate DDoS attack traffic in Q1–Q3



In Q3, the highest peak traffic of individual DDoS attacks reached 572.6 Gbps, which is higher than that in Q2 (445.7 Gbps) but lower than that in Q1 (615.1 Gbps).

Figure 3-2 Global trend of individual event peak traffic in Q1–Q3

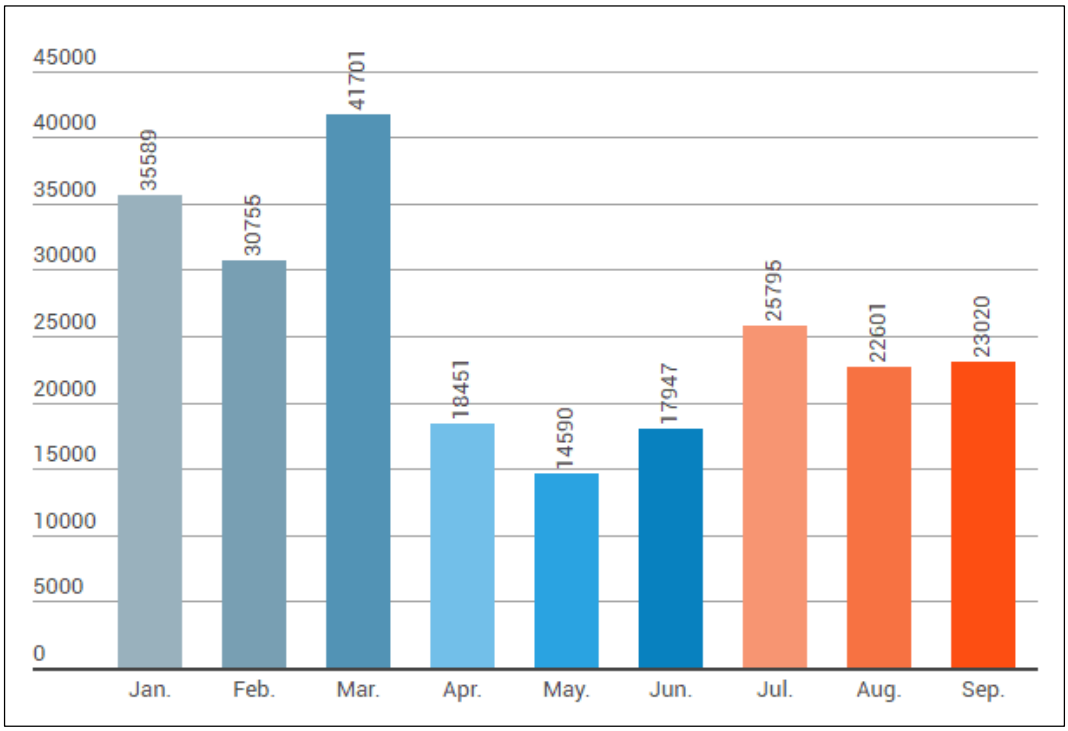


By tracing attack events with heavy traffic in Q3, we found that, except several NTP and SSDP reflection attacks, all non-reflection attacks involved IoT devices (such as web cameras and home routers) and most volumetric attacks were Mirai-based botnet attacks. This is a good demonstration of the viewpoint presented in the *NSFOCUS 2016 Security Report for Web Video Monitoring Systems* released on October 14: Currently, a great number of IoT devices have been infected with malicious botnets (such as Mirai and Luabot) and are exploited to perform hacker activities such as scanning and DDoS attacks. Generally, IoT devices are prone to various security issues. Therefore, compared with traditional PCs, hackers prefer to use IoT devices which are directly or indirectly exposed to the Internet as zombies controlled by their botnet. It can be predicted that, with the development of the IoT technology and increasing requirements of various industries, tens of thousands of IoT devices are connecting to the Internet at an alarming rate and this trend will be more obvious.

3.2 DDoS Attack Count

In Q3, we detected 71,416 DDoS attacks, which increased by 40% from Q2 (50,988) but was still lower than that in Ql (108,045). In July, there were 25,795 DDoS attacks in total, increasing by 43.7% compared with June. In August, the number of DDoS attacks decreased by 12.4% than that in July. In September, there were 23,020 DDoS attacks, on a par with August.

Figure 3-3 Monthly numbers of DDoS attacks in Q1–Q3

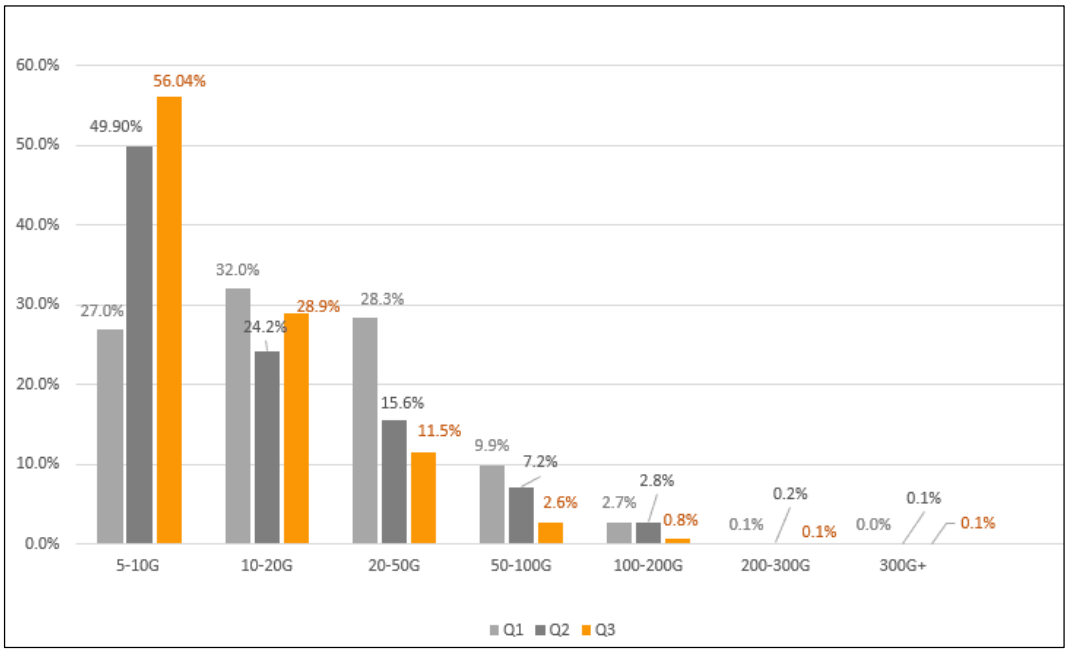


3.3 Attack Traffic Distribution

Compared with Q1 and Q2, the proportion of low-volume attacks with peak traffic of less than 20 Gbps accounted for 85% of the total attacks in Q3, down 10.8% and 26% respectively from Q1 and Q2.

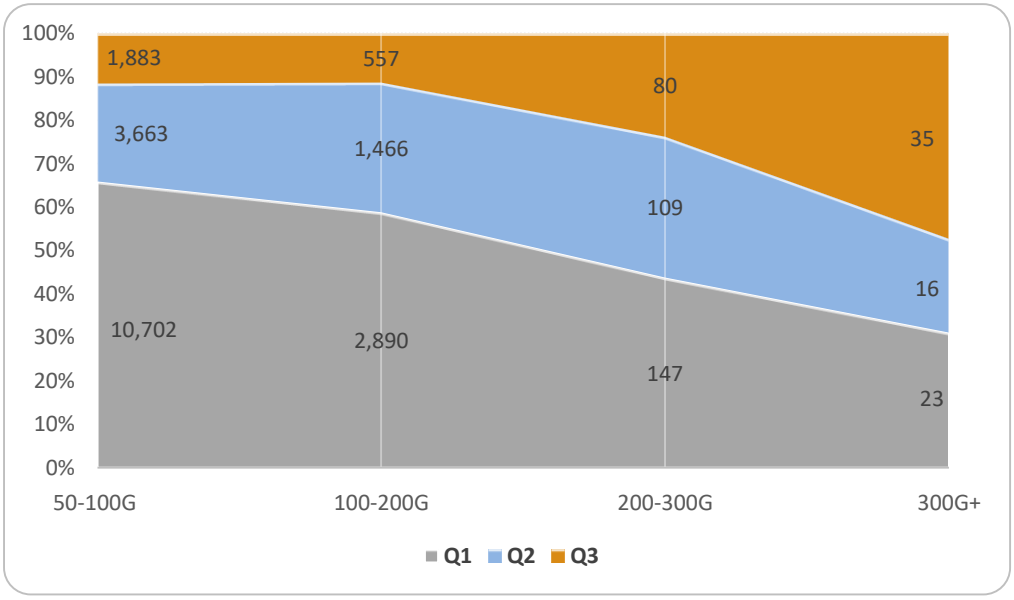
Attacks with peak traffic of 20–50 Gbps took up 11.5%, down 16.8% and 4.1% respectively from Q1 and Q2. Attacks with peak traffic of 50–300 Gbps accounted for 3.5%, down 9.2% and 6.7% respectively from Q1 and Q2. However, compared with those in Q1 and Q2, super high-volume DDoS attacks with peak traffic of over 300 Gbps increased.

Figure 3-4 Percentages of attack traffic in Q1–Q3



Compared with those in Q1 and Q2, super high-volume DDoS attacks with peak traffic of more than 300 Gbps increased, occurring 35 times in Q3. High-volume attacks with peak traffic of over 50 Gbps occurred 2555 times, respectively down 80% from Q1 (13,762 times) and 51% from Q2 (5254 times).

Figure 3-5 Attack counts of high-volume DDoS attacks (with peak traffic of over 50 Gbps) in Q1–Q3



4 Attack Duration and Repetition Frequency

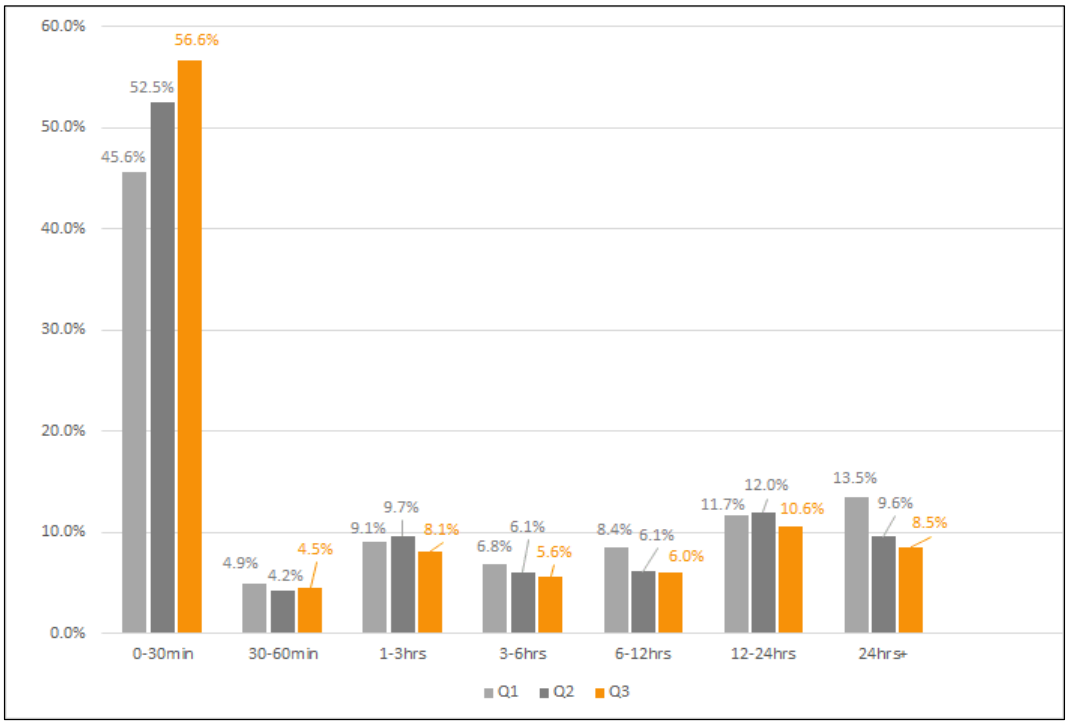
4.1 Attack Duration

In Q3, attacks lasting less than 30 minutes accounted for 56.6% of the total, a continuous increase from Q1 and Q2. The average attack duration was 7.2 hours, slightly decreasing from Q2 (8.1 hours)[①]. Attacks lasting more than 1 day accounted for 8.5% of the total, a continuous decrease from Q1 and Q2.

The most durable DDoS attack lasted 31 days and 19 hours (764 hours), generating 17 TB of traffic in total.

① We have improved the way of processing attack durations. Here, the data of Q1 and Q2 is processed with the new method, causing data differences from previous reports. The latest data prevails.

Figure 4-1 Percentages of attacks by attack duration in Q1–Q3

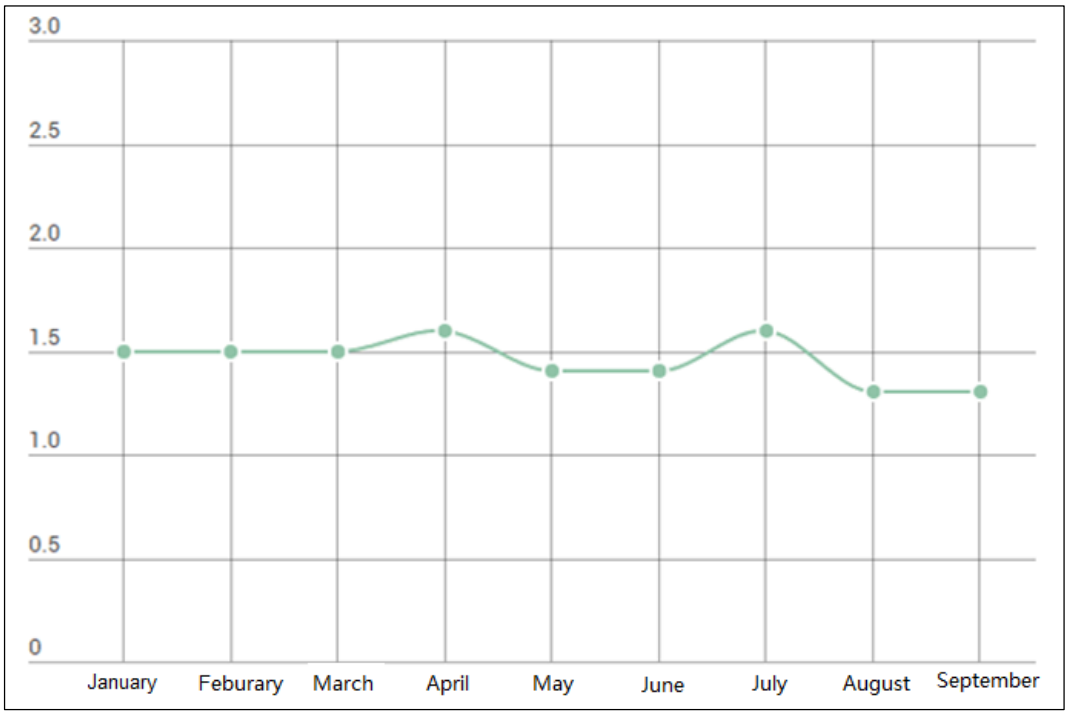


4.2 Repetition Frequency

In Q3, each IP address was attacked 1.4 times a month on average, which slightly decreased from Q1 and Q2 (both were 1.5 times).

In particular, we detected a network which was attacked 30 times by multi-vector attacks of short-time UDP flood and NTP reflection flood attacks.

Figure 4-2 Monthly attack counts of individual IP addresses in Q1–Q3



5 Attack Type Distribution

5.1 Attack Type Distribution by the Number of Occurrences and Traffic

From the perspective of the total number of occurrences, reflection attacks accounted for 90.5% of the total in Q3, up 20.6 percentage points from Q2. Among these reflection attacks, NTP reflection attacks occurred most frequently, which accounted for 40.4% and was followed by CHARGEN reflection attacks, SSDP reflection attacks, and SNMP reflection attacks.

In a reflection attack, an attacker spoofs the IP address of a victim as the source request address and sends it to a large number of reflectors prone to a protocol vulnerability. The bytes of response packets are far more than those of request packets. In this case, the traffic is magnified, forming a high-volume DDoS attack against the target network. Unlike botnet attacks, reflection attacks are less than costly than traditional DDoS attacks because they do not need to infect and control a large number of attack sources in advance. Currently, the reflection attack type with the biggest amplification factor is NTP reflection attack, which has an amplification factor of up to 556.9.

Figure 5-1 Attack type distribution by the total number of occurrences

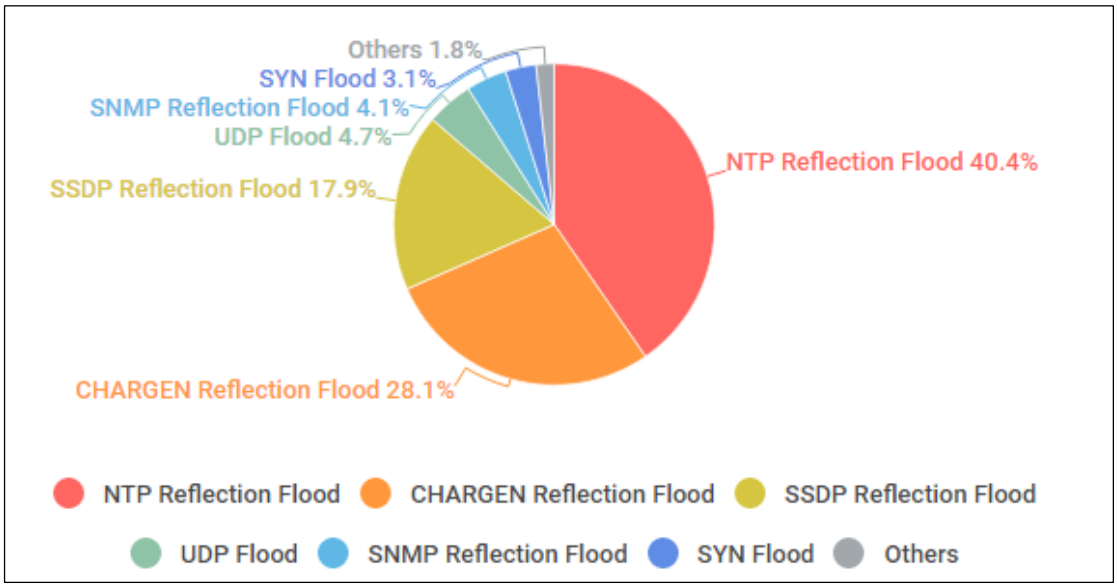
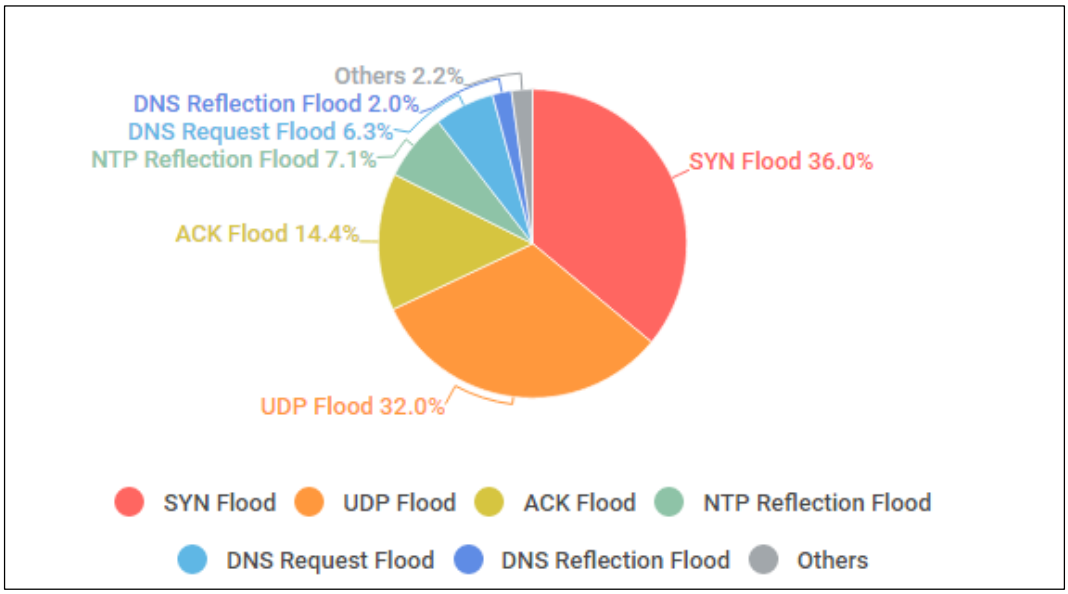


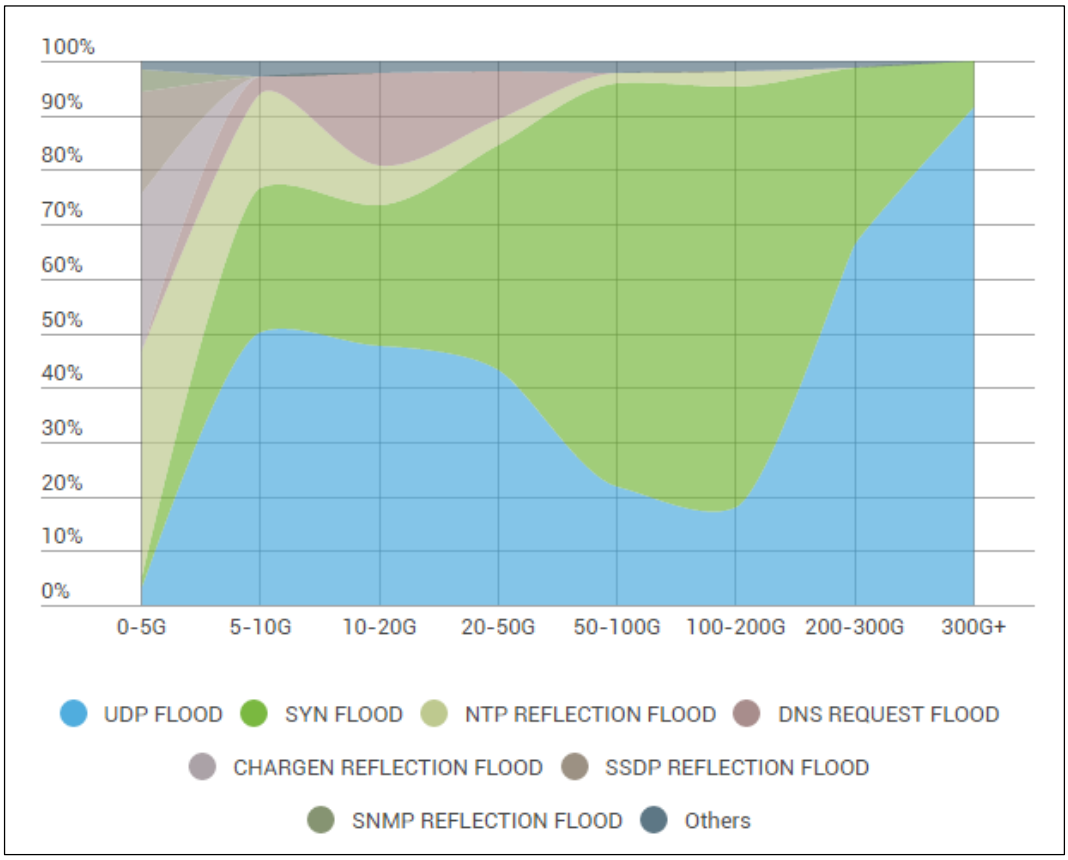
Figure 5-2 Attack type distribution by total traffic



5.2 Attack Type Distribution by Traffic

According to our analysis, the distribution of attack protocol types varies with peak attack traffic. Among low-volume attacks with peak traffic of less than 5 Gbps, NTP reflection flood attacks and CHARGEN reflection flood were rather frequently seen; among medium-volume attacks with peak traffic of 50–200 Gbps, SYN flood attacks showed the most activity; among medium- and low-volume attacks with peak traffic of 5–50 Gbps, high-volume attacks with peak traffic of over 200 Gbps, and super high-volume attacks, UDP flood attacks showed the most widespread presence, followed by SYN flood attacks. This suggests that attack methods and capabilities vary with attack tools, botnet types, and attack organizations.

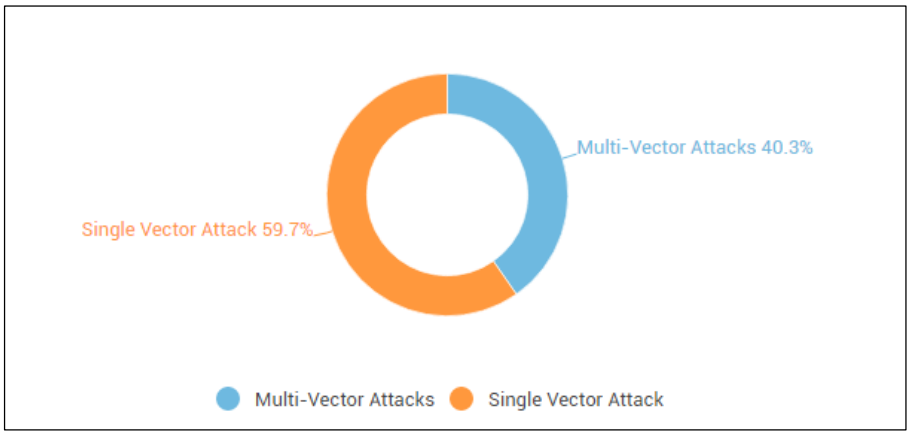
Figure 5-3 Attack type distribution by traffic



6 Multi-Vector Attacks

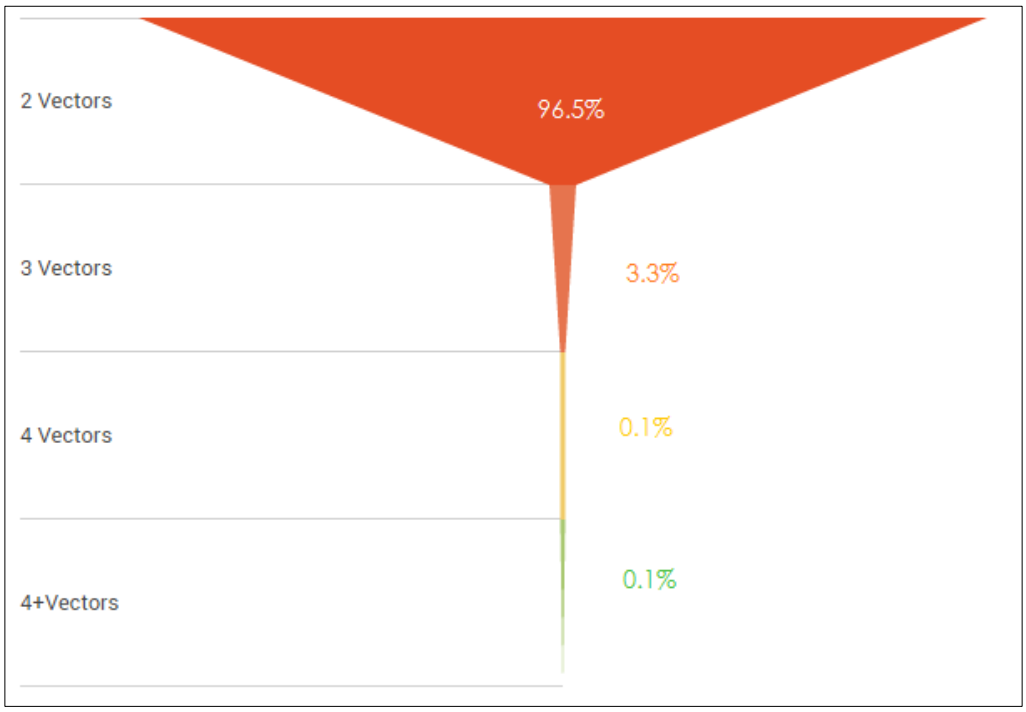
In Q3, the proportion of attacks characterized by mixed types of traffic accounted for 40.3% of the total attacks, 6.6 percentage points higher than Q2 (33.7%).

Figure 6-1 Proportion of multi-vector attacks and that of single-vector attacks



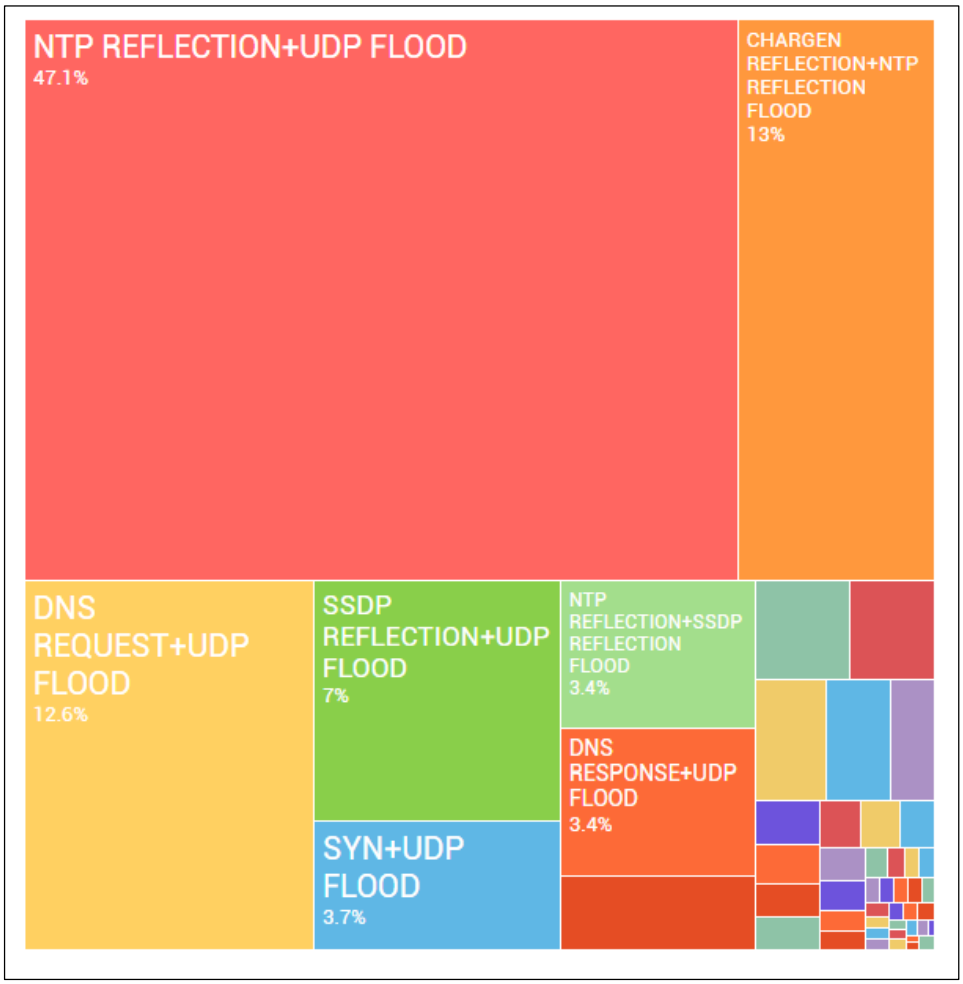
Analyzing the number of vectors used in multi-vector attacks, we found that most frequently such attacks were launched by means of two or three vectors, accounting for 99.8% of the total multi-vector attacks, as shown in the following figure.

Figure 6-2 Proportions of attacks with different numbers of vectors



In addition, we analyzed flood combinations in multi-vector attacks, trying to figure out which combination was most frequently used by attackers. Figure 6-3 shows the analysis result.

Figure 6-3 Proportions of multi-vector attacks with different flood combinations



Most frequently, a multi-vector attack in Q3 was made up of the NTP reflection flood and UDP flood. Such attacks accounted for 47.1% of the total multi-vector attacks in Q3. Reflection attacks were still popular among attackers, accounting for a large proportion. CHARGEN reflection + NTP reflection flood, SSDP reflection + UDP flood, and NTP reflection + SSDP reflection are common combinations.

7 Reflection Attacks

7.1 Proportions of Various Reflection Attacks

In Q3, reflection attacks were still in the wild, occurring much more frequently than in Q2. We analyzed the number and traffic proportion of each reflection attack type and had the following findings:

In terms of attack traffic, NTP reflection flood attacks generated the largest volume of traffic, accounting for 60.5% of the total reflection attack traffic, 24.4 percentage points higher than that in Q2. DNS reflection and SSDP reflection flood attacks came in second and third, with related traffic taking up 19.6% and 5.9% respectively, a bit lower than in Q2.

In terms of the number of occurrences, NTP reflection flood overtook CHARGEN reflection flood to become the most active reflection attack, accounting for 42.6% of the total, 13.6 percentage points higher than in Q2. In contrast, Q3 saw a slight decline in proportions of CHARGEN reflection flood and SSDP reflection flood attacks.

Figure 7-1 Proportions of reflection attack types in terms of attack traffic

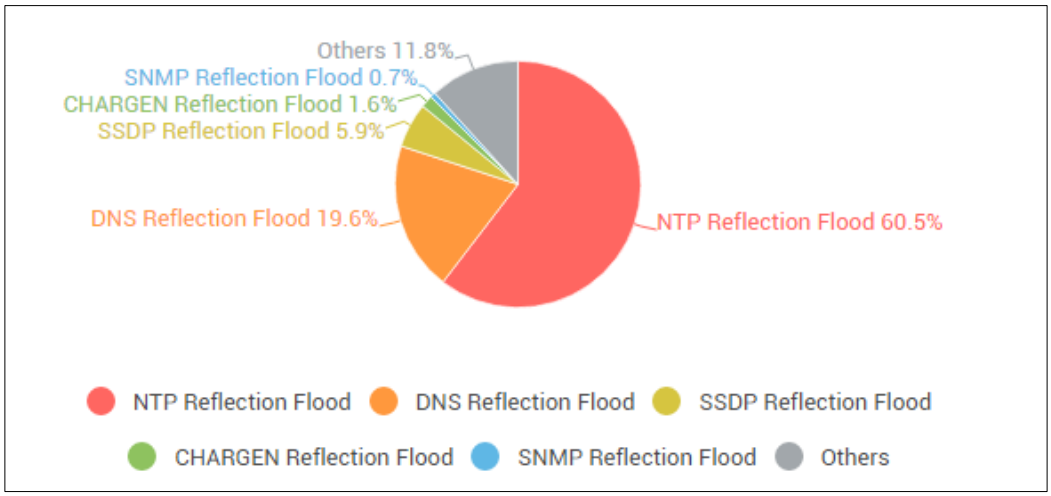
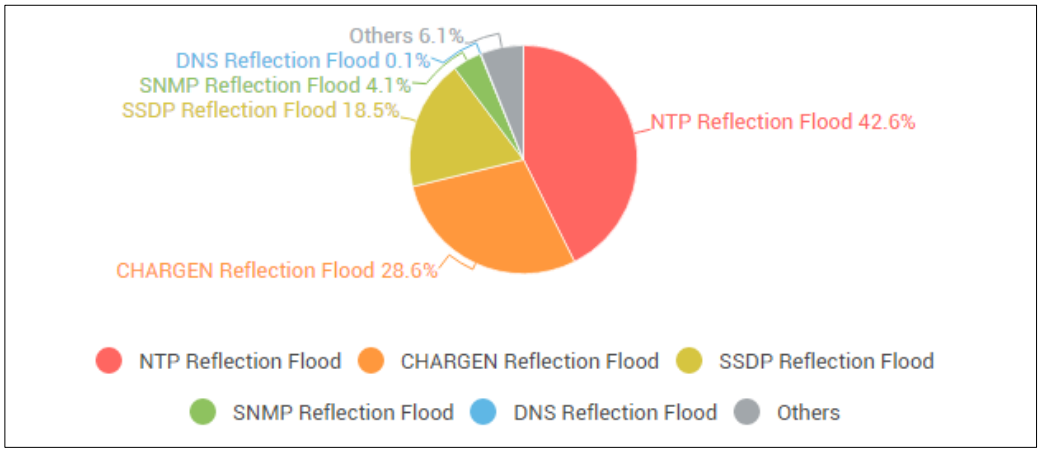


Figure 7-2 Proportions of reflection attack types in terms of the number of occurrences



7.2 Global Distribution of Active NTP Reflectors

According to our latest statistics, the number of reflectors used for launch of NTP reflection flood attacks in Q3 reached 25,371, a 440% increase compared with Q2. Figure 7-3 shows the global distribution of these reflectors. Among all these countries, China had the largest proportion of reflectors, followed by the US, Vietnam, South Korea, and Russia.
Compared with Q2, Vietnam and South Korea saw an increase in the proportion of reflectors, overtaking Russia, Japan, and France to make it into top 5.

Figure 7-3 Global distribution of NTP reflectors used in reflection attacks

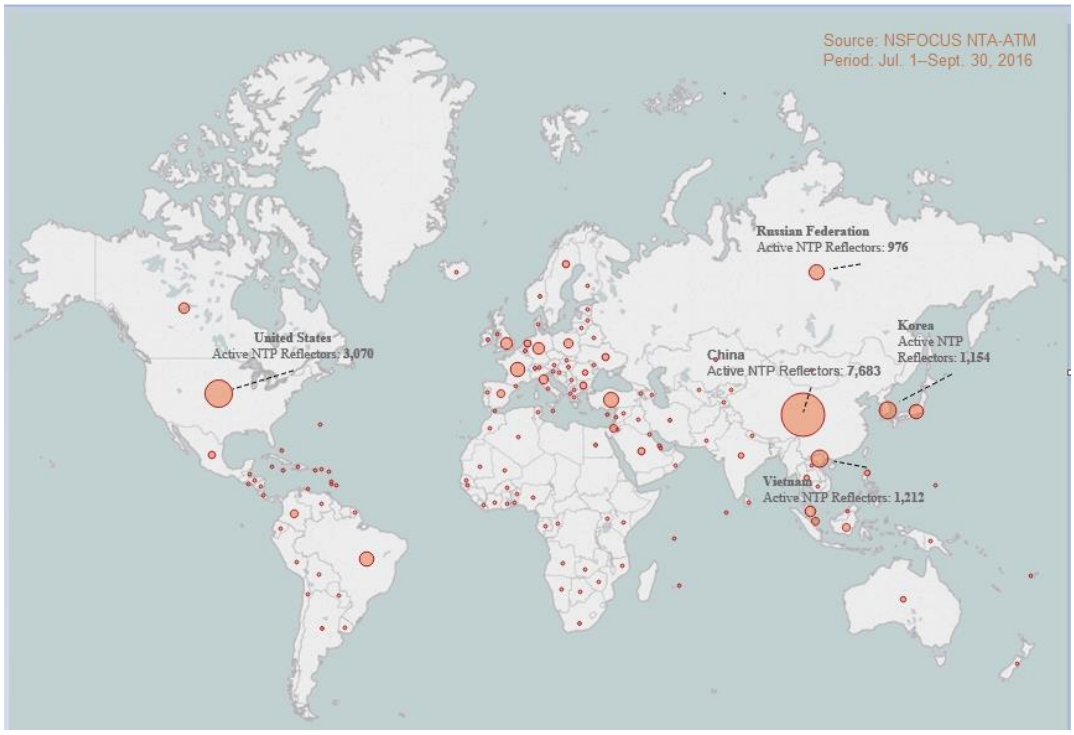
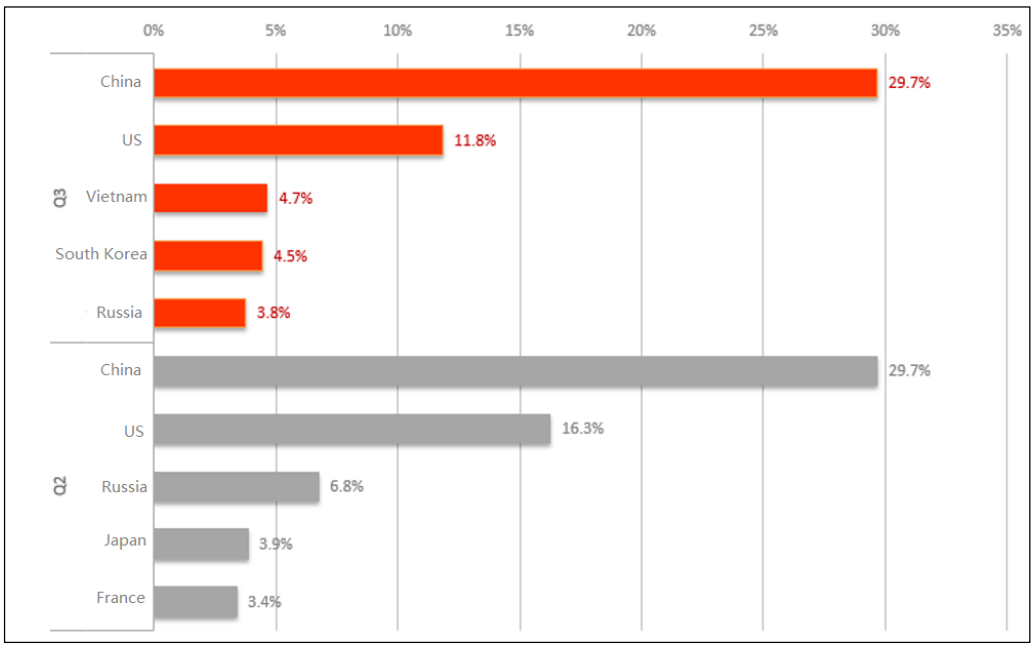


Figure 7-4 Comparison of top 5 countries in Q2 and Q3 in terms of the proportion of NTP reflectors



8 DDoS Attack Trend: IoT Device-based Botnets

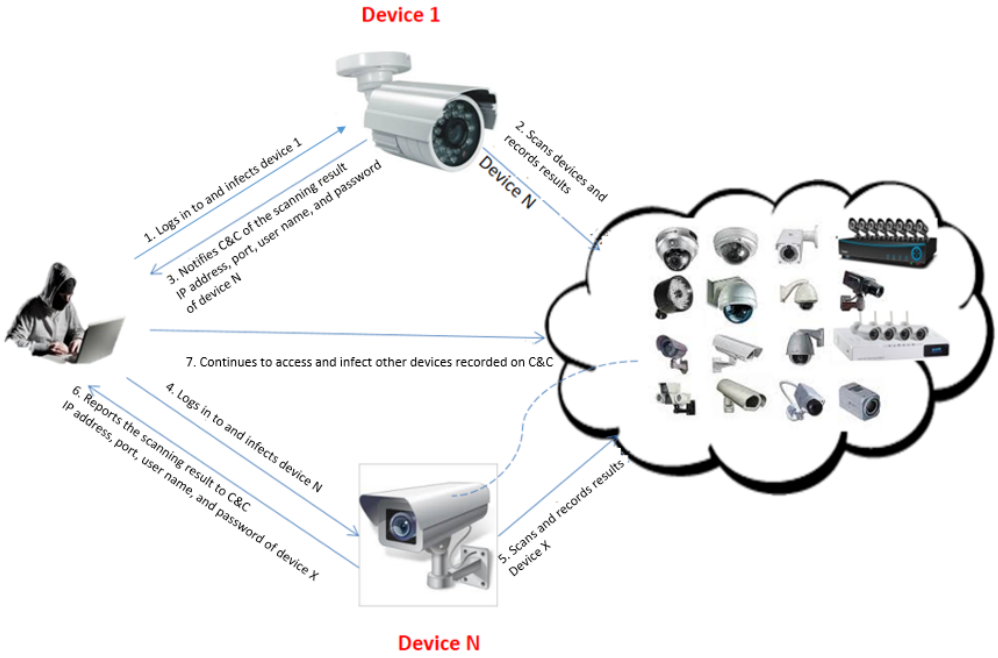
In the *NSFOCUS 2016 Security Report for Web Video Monitoring Systems* released on October 14, we analyzed the security status of web video monitoring systems (WVMS) as a typical type of IoT devices and WVMS-based botnets in an all-round manner. The report points out that a large number of IoT devices have been infected with malicious bot programs worldwide, including notorious LizardStresser, recently famed Mirai, and emerging malware Luabot. These infected devices constitute huge IoT botnets, which are controlled by various hacker organizations to perform hacker activities such as scanning and DDoS attacks. Only one week after the report was released, the Internet across most parts of the US was paralyzed on the morning of October 21 (Eastern Time). Many well-known websites, including PayPal, Twitter, GitHub, and Amazon, were affected. It was reported that this accident was caused by a DDoS attack targeting Dyn, a DNS service provider. According to Dyn, the attack was initiated by millions of Mirai-infected IoT devices like web cameras. If that is the case, Mirai, an IoT-based botnet, succeeded in launching another attack with an extensive influence in the wake of DDoS attacks targeting Krebs on Security and OVH. By far, there have been many speculations and interpretations on how the attack was executed to cause such extensive network outage. Dyn is expected to provide more detailed data on the attack[②]. Anyway, IoT-based botnets have changed the global trend of DDoS attacks. They have quickly gained favor from hackers for launching DDoS attacks. Their potential to cause devastating damage should never be underestimated. The current trend of IoT-based botnets, especially the activities of Mirai, will be analyzed in detail in the following sections.

8.1 How an IoT-based Botnet Works

Analyzing the infection and spread means of IoT-based botnets, we found that usually such an attack was conducted as follows: An attacker first obtains the shell privilege of an IoT device by exploiting a high-risk vulnerability or cracking a weak password. Then the attacker plants malware into the device and uses the infected device to further scan and attempt to log in to other devices. Information about those devices that can be successfully accessed is sent to the C&C control end, from which the malware is spread or downloaded by the script planted in devices. In this way, a multitude of IoT devices around the globe are continuously infected.

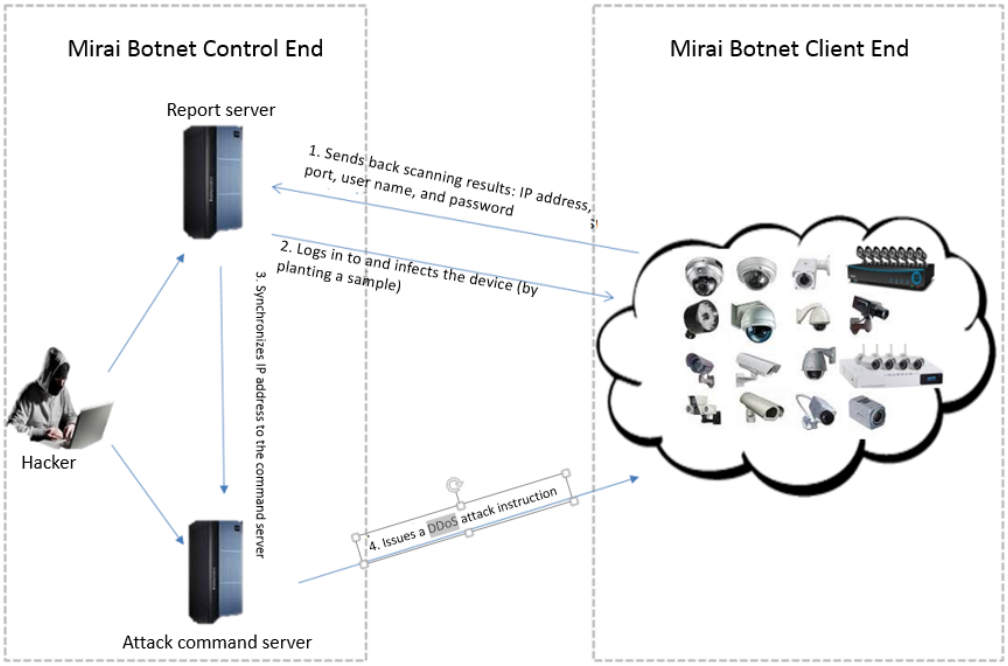
② The latest statement of Dyn is available at http://dyn.com/blog/category/press-releases-news-company-updates/

Figure 8-1 Infection and spread means of a bot program



Take Mirai, the most active bot program, as an example to show how the main control end of a botnet communicates with bots. Botnet control terminals play roles of two types of servers: One is called the command server used for issuing DDoS instructions and scanning instructions to bots; the other is called the report server used for receiving scanning results from bots and planting malware into target devices in addition to storing malicious samples. The two types of servers use different ports to communicate with bots. Figure 8-2 shows the procedure of communication between the botnet control end and bots.

Figure 8-2 Procedure of communication between the Mirai botnet control end and bots



8.2 DDoS Attack Capability of IoT-based Botnets

The most important function of a botnet is use by hackers for launching DDoS attacks or provisioning of the DDoS rental service. There are numerous IoT devices around the world that contain high-risk vulnerabilities such as weak passwords. These devices stay online without being attended and are generally allocated high bandwidths, making them the optimal target of compromise for botnets. This is also the reason why an IoT-based botnet can easily initiate attacks with peak traffic reaching 1 Tbps without using any reflective amplification protocols.

In addition, IoT-based botnets employ attack approaches as effective as, if not more sophisticated than, traditional DDoS tools.

Besides DDoS attacks characterized by spoofed source IP addresses, application-layer attacks launched from real source IP addresses are made possible by botnets, which can even break through protections of certain security devices. For example, some malicious samples can implement the three-way handshake and contain many common referer and user-agent fields for launching HTTP GET/POST attacks. During the attack, random referer and user-agent values are used to evade detection from security devices, as shown in Figure 8-3. Luabot has a built-in V7 JavaScript engine to bypass JavaScript-based protection mechanisms such as Cloudflare and Sucuri.

Figure 8-3 Malicious sample containing referer and user-agent fields for application-layer DDoS attacks

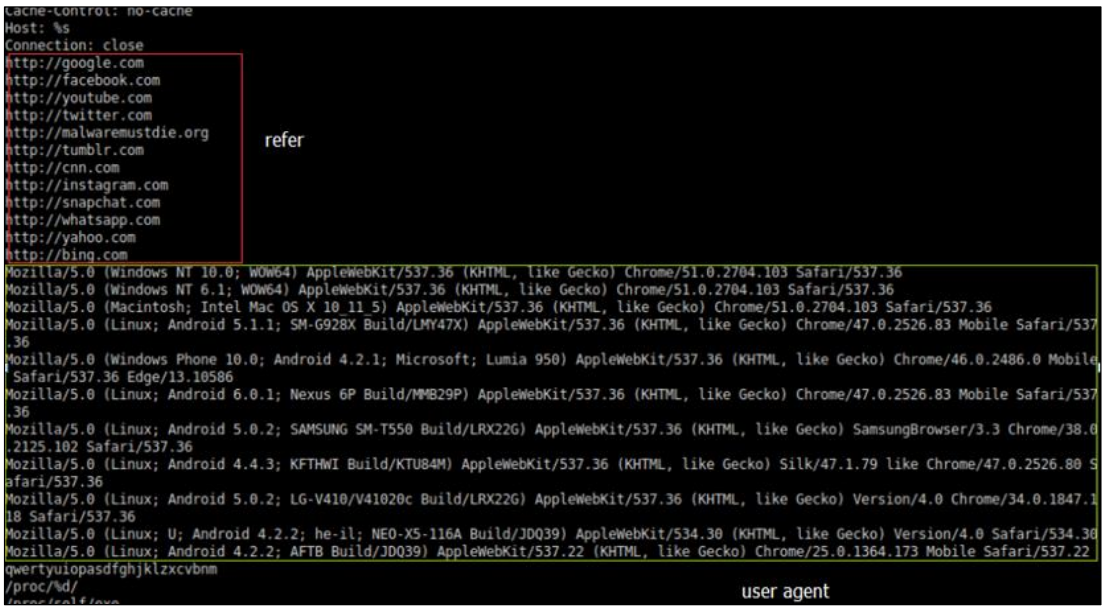
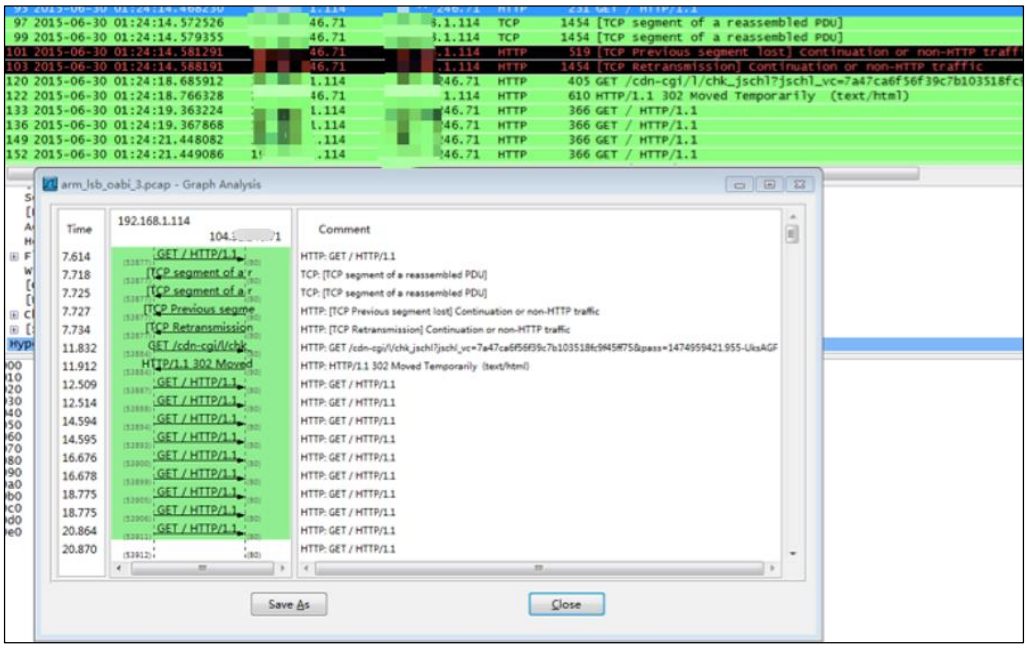


Figure 8-4 Packet captured during a Luabot attack that breaks through Cloudflare protection



8.3 Distribution of Main Control Terminals of Mirai Botnets

By the end of October, we had independently detected 23 main control terminals for Mirai botnets. Table 8-1 lists command servers, report servers, communication ports used by these two types of servers, registration date, and update date.

Table 8-1 Main control terminals for Mirai botnets

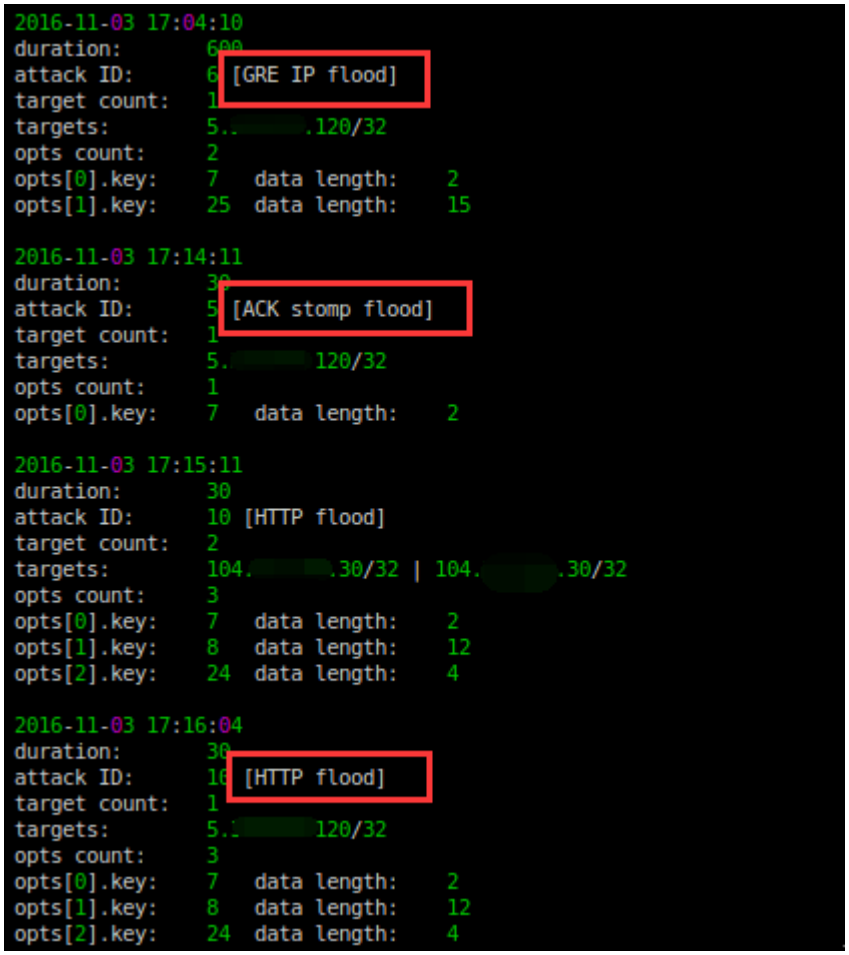
Attack Command Server - Addr	Attack Command Server - Port	Report Server - Addr	Report Server - Port	Registration Date	Update Date
gay.c[redacted].racing	23	report.[redacted].racing	48101	May 28, 2016	
fucklu[redacted]t.com	23	lua.f[redacted].com	48101	Jul. 26, 2016	
laatm[redacted]h.cf	23	repo[redacted]h.cf	48101	Nov. 16, 2015	
im.[redacted].work	1367	youre.[redacted].work	48202	Oct. 16, 2016	
lol.dis[redacted].racing	23	dongs.[redacted].racing	48101	May 28, 2016	
swing[redacted].ru	23	new.s[redacted].ru	48101	Aug. 22, 2016	
swin[redacted]e.ru	23	swir[redacted].ru	48101	Nov. 18, 2014	Jun. 13, 2016
tw.s[redacted].com	23	tw.s[redacted].com	48101	Feb. 9, 2016	Oct. 13, 2016
fuck1.ba[redacted].com	23	fuck.b[redacted].com	53	Feb. 9, 2016	
network.santasbigcandycane.cx	23	report.santasbigcandycane.cx	48101	Sept. 15, 2016	
heis[redacted].work	23	sheis[redacted].work	48202	Oct. 16, 2016	
hight[redacted].club	666	report.h[redacted].club	48101	Oct. 24, 2016	
ftp.xer[redacted].xyz	23	listen.xer[redacted].xyz	48101		
sdrfa[redacted].top	23	sdrfat[redacted].top	48101	Oct. 27, 2016	
cnc.d[redacted].racing	23	report.d[redacted].racing	48101	May 28, 2016	
kankerc.[redacted].xyz	23	report.q[redacted].xyz	48101		
securi[redacted].us	23	rep.se[redacted].us	4810	Sept. 4, 2016	
loads[redacted].pw	23	r.lo[redacted].pw	37065		
6d77a[redacted]net	2047	e98d[redacted].net	20470	Apr. 22, 1999	May 26, 2016
q5f2k0e[redacted].ru	23	xg5kisn74mk2[redacted].ru	48101	Oct. 28, 2016	
ne[redacted].org	23	report.[redacted].org	48101	Mar. 25, 2016	
www.mu[redacted].org	23	www.m[redacted].org	4810	Sept. 20, 2016	
our[redacted].ru	23	repor[redacted].ru	48101	Aug. 19, 2016	

From dates disclosed, we can see most servers were registered or updated after May, particularly in the period from the end of July to the end of October, during which Mirai happened to be most active. santasbigcandycane.cx is the main control terminal mentioned in the source code of Mirai.

Keeping a close eye on these botnets, we find that some control terminals cannot be connected although many are still active as of the date when this report is finished. We guess this is because organizations have taken actions to tackle Mirai in response to frequent reports of high-volume DDoS attacks associated with Mirai.

The following figure shows attack commands detected by our security device: The botnet q5f2k0exxxx.ru launched three waves of DDoS attack on the same target in a short time with varied attack approaches, namely, GRE IP flood, ACK stomp flood, and HTTP flood. This is probably because the attacker was trying to find out the maximum bandwidth and defense capability of the target network.

Figure 8-5 DDoS attack commands issued by a main control terminal of a Mirai botnet



What also needs to be noted is that attackers often change IP addresses of main control terminals to evade security checks. According to IP addresses found in the last round of attack, the main control terminals were mainly located in Europe (Holland, France, Poland, and Ukraine), US, and Japan.

8.4 Distribution of Mirai Bots

By the end of October, the number of IoT devices infected with Mirai reached 1,508,059, distributed in 209 countries and regions. Figure 8-6 shows the global distribution of Mirai bots.

Figure 8-6 Global distribution of Mirai bots

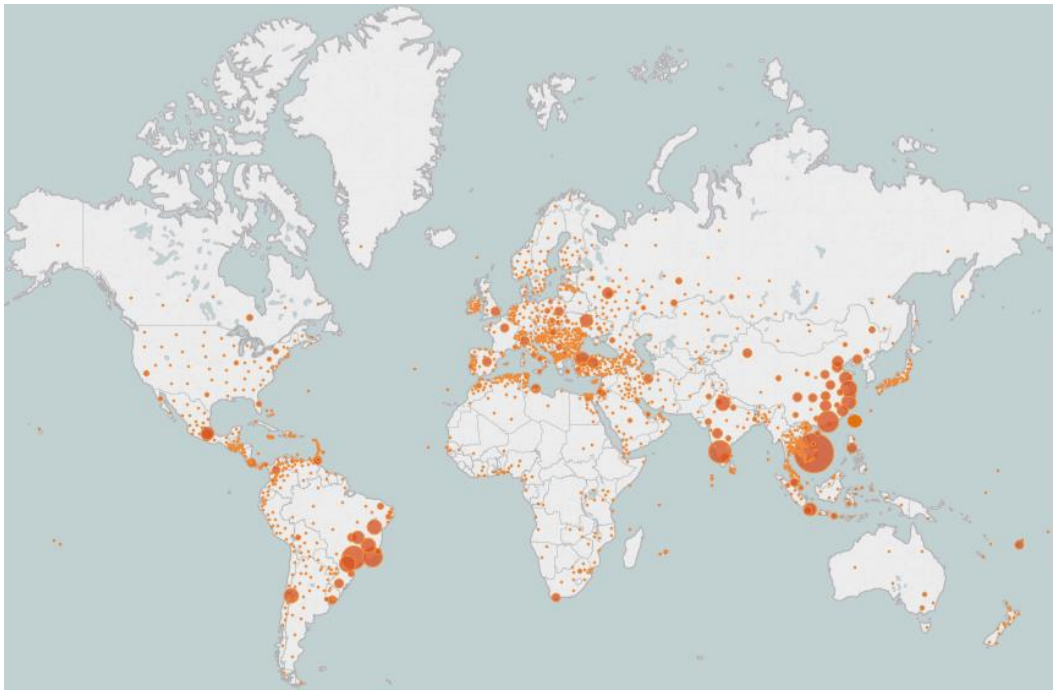
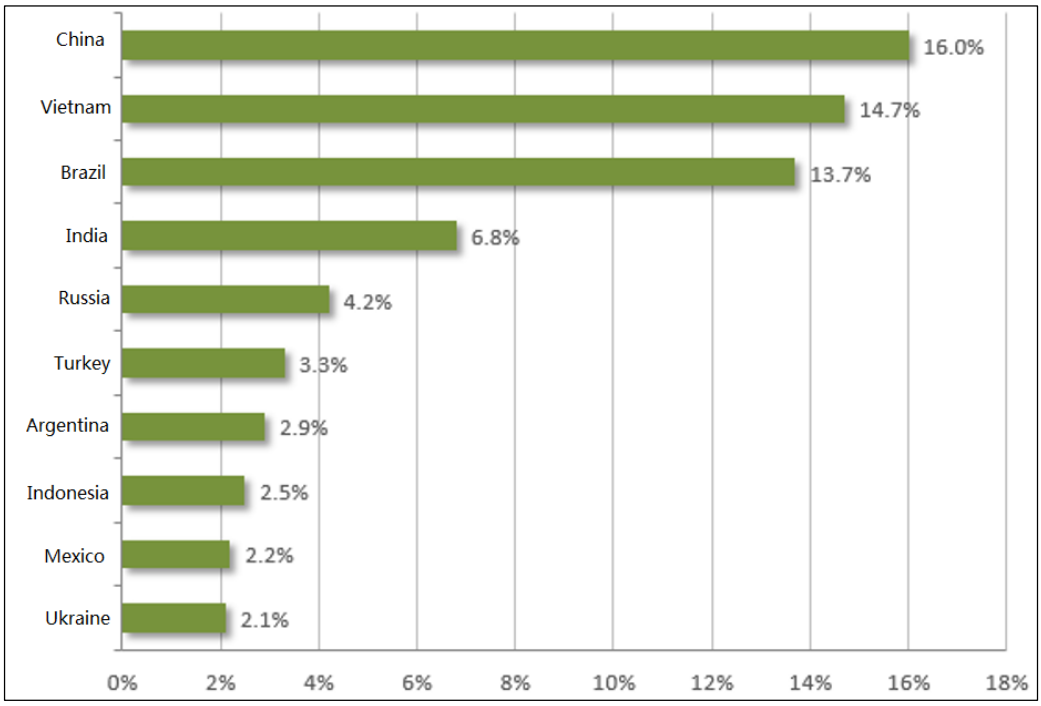


Figure 8-7 shows top 10 countries with the greatest number of Mirai bots. China, Vietnam, and Brazil are the three countries most severely affected, with 16%, 14.7%, and 13.7% of Mirai bots respectively. Other countries on the top 10 list are India, Russia, Turkey, Argentina, Indonesia, Mexico, and Ukraine. Mirai bots in these 10 countries take up 68.4% of the global total.

Figure 8-7 Distribution of Mirai bots in top 10 countries

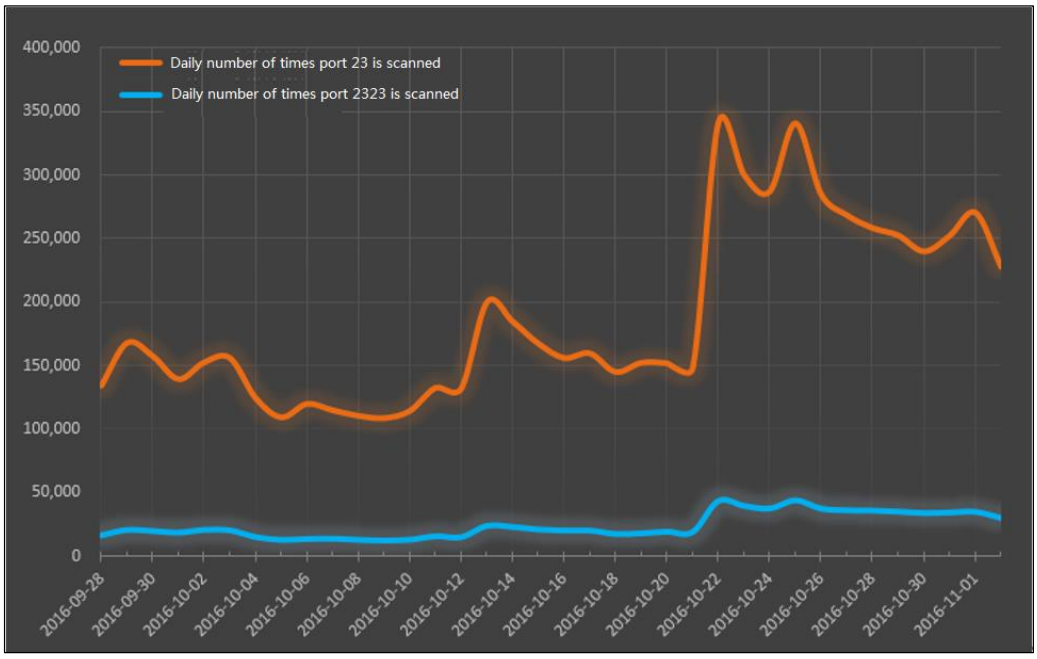


8.5 Scanning Activities of Mirai

At the end of September, the author or Mirai released the source code of the malware. Through analysis, we found that Mirai botnets scanned ports 23 and 2323 by using a fixed signature, in a bid to find new infection targets on the network. Therefore, we started to monitor scanning activities targeting these two ports around the world. Figure 8-8 shows two curves indicating the number of times ports 23 and 2323 have been scanned in the last month (Eastern Time). Before October 22, port 23 was scanned about 150,000 times a day and port 2323 about 20,000 times a day. On October 22, the number of scans targeting port 23 rose significantly to 340,000 a day and in the following several days, this number fluctuated, showing a general trend of slow decline. On the same day, the number of times port 2323 was scanned doubled. We think that the sudden rise in the number of scans on October 22 may be associated with the fact that Dyn ascribed the extensive outage in USA on August 21to Mirai, bringing Mirai into the spotlight, and many hackers, on hearing the news, began to use Mirai to create their own botnets.

Although the number of scans lowered a bit after October 22, it was still higher than that detected before October 22. From observation, we find that Mirai botnets remained active in the last month. It is foreseeable that the number of IoT devices infected with Mirai and its variants will soar as more and more such devices keep connecting to the Internet worldwide.

Figure 8-8 Daily number of times ports 23 and 2323 were scanned by Mirai botnets



Just as we mentioned in the *2016 NSFOCUS Security Report Regarding Network Video Surveillance Systems*, if the current security status of the IoT fails to be controlled and changed, IoT-based botnets will grow at an astonishing pace, posing a great challenge to cybersecurity around the globe.

9 Epilog

With the rise of the IoT and various security issues exposed currently, the global DDoS attack trend is undergoing a gigantic change implemented in three phases: Initially, DDoS attacks were mainly launched with botnets composed of traditional PCs; the past two years witnessed the prevalence of reflective amplification attacks; now attackers turn their eyes to botnets made up of various IoT devices. This change reflects the fact that attackers, driven by interests, keep seeking cost-efficient attacks tools and vectors. With a view to promoting the sound and orderly development of the Internet ecology, we will keep a close eye on the ever changing DDoS attack trend and release warnings and provide effective defense mechanisms in time. This a goal we have been making unremitting efforts to achieve.

Special Statement

All data for analysis is anonymized and no customer information appears in this report to avoid information disclosure by negligence on our part.

NSFOCUS DDoS Defense Research Lab and Threat Response Center (TRC) are keeping a close eye on the progress of DDoS attack events. For more information, please contact

- NSFOCUS by Sina Weibo at:
- http://blog.nsfocus.net/
- NSFOCUS TRC by Sina Weibo at:
- http://weibo.com/threatresponse
- NSFOCUS by finding:
- NSFOCUS at WeChat

To learn more:

1. About *NSFOCUS Q2 2016 Report on DDoS Situation and Trends*, please visit:

http://blog.nsfocus.net/nsfocus-2016-q2-ddos-situation-report/

2. About *NSFOCUS 2016 Security Report for Web Video Monitoring Systems*, please visit:

http://blog.nsfocus.net/nsfocus-2016-network-video-surveillance-system-security-report/

3. About *NSFOCUS Q1 2016 Report on DDoS Situation and Trends*, please visit:

http://blog.nsfocus.net/nsfocus-2016-q1-ddos-situation-report/

4. About *NSFOCUS 2015 DDoS Threat Report*, please visit:

http://blog.nsfocus.net/2015-annual-ddos-threat-report/