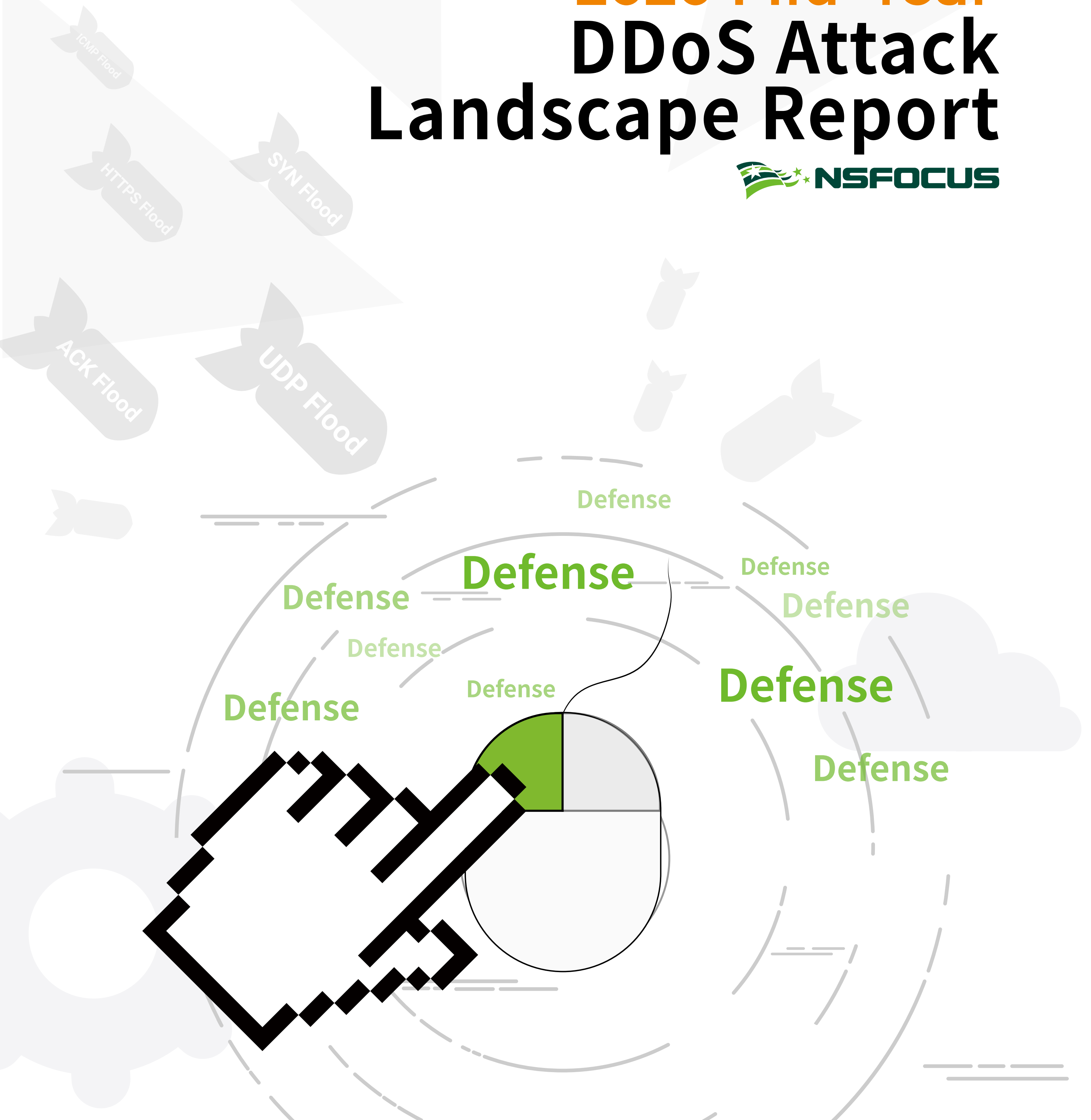
2020 Mid-Year DDoS Attack Landscape Report

NSFOCUS



NSFOCUS

About NSFOCUS

NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide multi-layered, unified and dynamic protection against advanced cyber attacks.

NSFOCUS works with Fortune Global 500 companies, including four of the world's five largest financial institutions, organizations in insurance, retail, healthcare, critical infrastructure industries as well as government agencies. NSFOCUS has technology and channel partners in more than 60 countries, is a member of both the Microsoft Active Protections Program (MAPP), and the Cloud Security Alliance (CSA).

A wholly owned subsidiary of NSFOCUS Technologies Group Co., Ltd., the company has operations in the Americas, Europe, the Middle East and Asia Pacific.

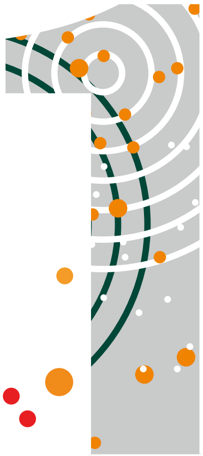
Special Statement

All data used for analysis has been anonymized and no customer information appears in this report to avoid information disclosure per GDPR.

CONTENTS

Summary

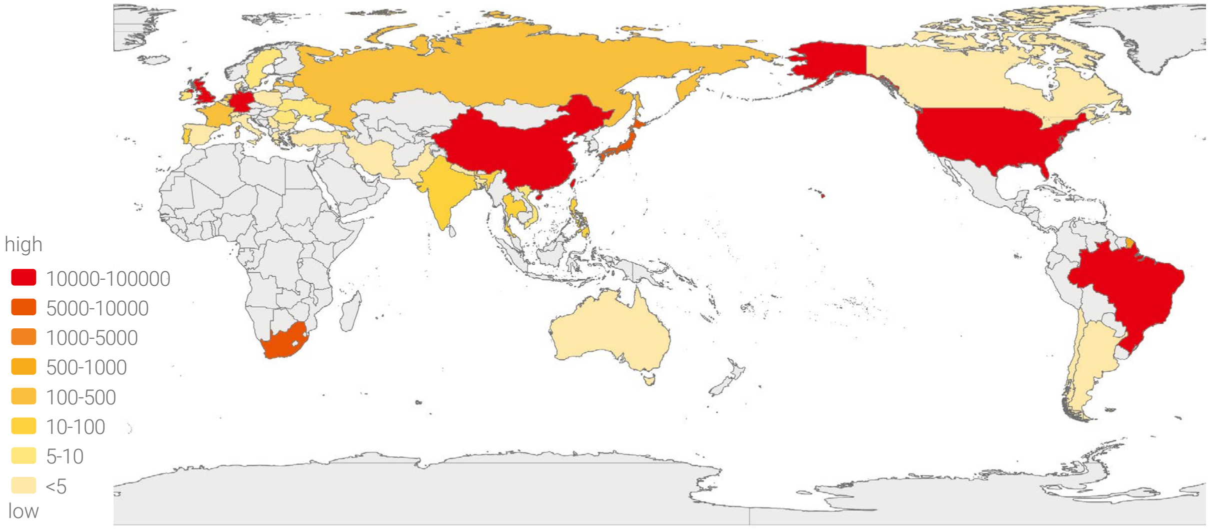
1. **Global distribution of DDoS attacks:** U.S. suffered the most DDoS attacks, and Japan received the largest volume of DDoS traffic.
2. **DDoS attack trend:** March and April witnessed the most frequent DDoS attacks, and May saw the peak of attack traffic.
3. **DDoS attacks and COVID-19 pandemic:** DDoS attacks fluctuated noticebly with the worldwide outbreak of the COVID-19 pandemic. Germany and the U.S. were two typical examples.
4. **Attack lethality:** Compared with the first half of 2019, the first half of 2020 experienced a decline in the number of attacks withincreasing magnitute.
5. **Attack types:** SYN flood and UDP flood remained dominant DDoS attacks.
6. **Attack duration:** Short-duration and effective attacks were the norm, with 68% of the attacks lasting less than 5 minutes.
7. **Attack peak:** May was exposed to the strongest attack, with the peak reaching 634.6 Gbps.
8. **Attack gangs:** Among the 15 IP gangs under our continuous monitoring in the first half of 2020 , the largest attack utilized 217,000 attack sources.



Global distribution of DDoS attacks: U.S. suffered the most DDoS attacks, and Japan received the largest volume of DDoS traffic.

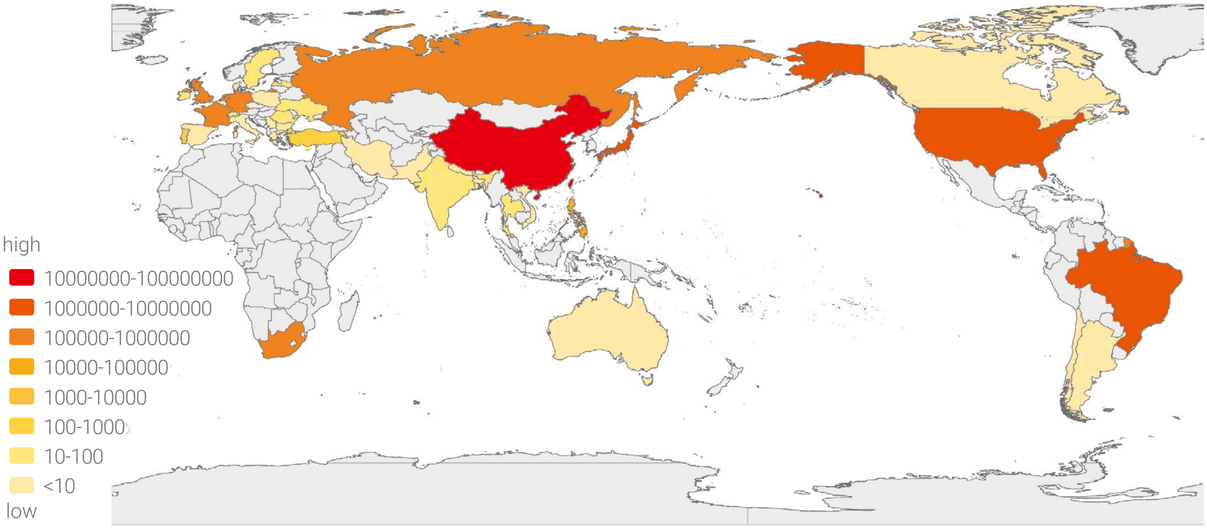
The following figures displayed the global distribution of DDoS attacks and that of DDoS attack traffic. In the first half of 2020, the USA suffered the most DDoS attacks, accounting for 34.15%. Japan received the largest volume DDoS traffic, accounting for 49.11%.

Global Distribution of DDoS Attack Events



Target Country	Attack Count	Percentage
United States	59,080	34.15%
United Kingdom	51,053	29.51%
China	18,961	10.96%
Germany	14,780	8.54%
Brazil	13,024	7.53%
Japan	9208	5.32%

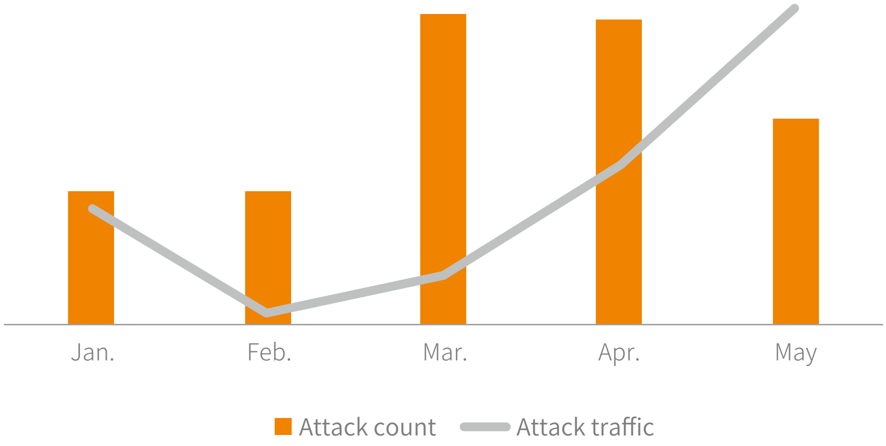
Global Distribution of DDoS Attack Traffic



Target Country	Attack Count	Percentage
Japan	25,949,768	49.11%
China	12,094,545	22.89%
United States	8,001,844	15.14%
Brazil	4,279,189	8.10%
Germany	969,778.9	1.84%
France	454,958.9	0.86%

DDoS attack trend: March and April witnessed the most frequent DDoS attacks, and May saw peak of attack traffic.

Number and Traffic of DDoS Attacks

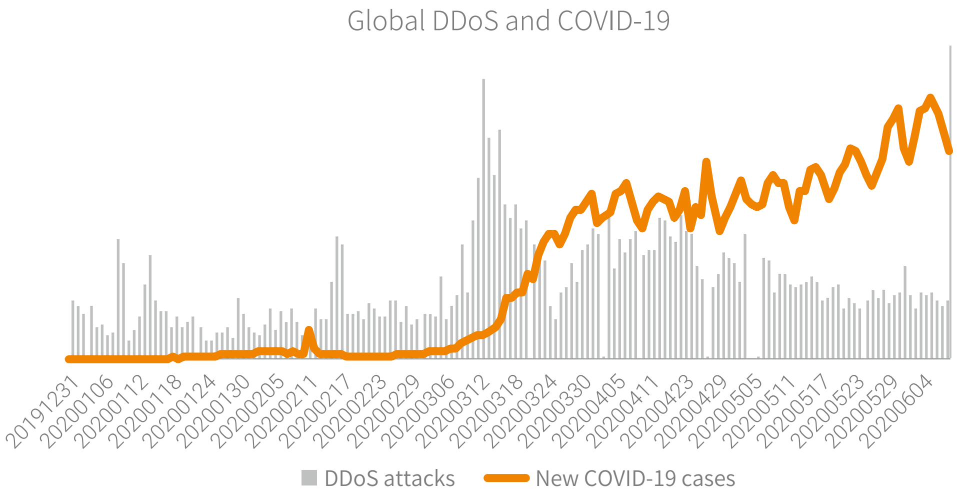


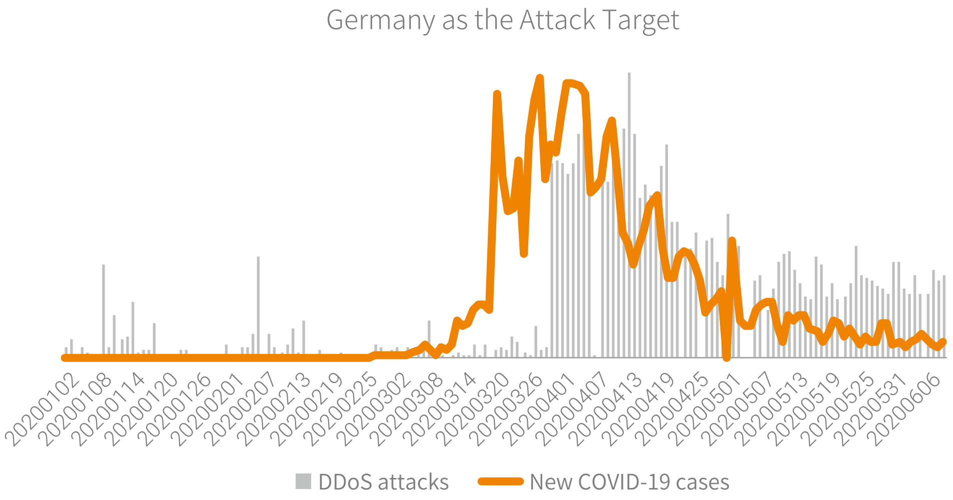
DDoS attacks and COVID-19 pandemic: DDoS attacks fluctuated noticebly with the worldwide outbreak of COVID-19. Germany and the U.S. were two typical examples.

DDoS attacks and COVID-19 pandemic: DDoS attacks fluctuated noticebly with the worldwide outbreak of the COVID-19 pandemic. Germany and the USA were two typical examples. Interestingly, DDoS attacks soared in Germany after the pandemic outbreak, while the U.S. saw the sharpest rise in DDoS attacks when the number of newly confirmed COVID-19 cases began to surge.

Globally, March and April witnessed the pandemic spreading most rapidly and DDoS attacks taking place most frequently. As a result of worldwide pandemic spread, people had an increasing reliance on the Internet for their social activities and day-to-day work. The surge in DDoS attacks during the pandemic outbreak was partly attributed to competition between peers, where a company attempted to take down another by paralyzing the latter's network with DDoS attacks to such an extent as to disrupt its normal operations. In addition, network law enforcement agencies loosened supervision, while many attackers had more time on their hands because of not needing to commute to work as usual and so could take their time to launch more illegal attacks for profits.

Below are the trend charts of the number of global DDoS attacks and that of newly confirmed COVID-19 cases. On March 11, the World Health Organization (WHO) announced the COVID-19 epidemic as a global pandemic, and a spurt occurred in confirmed cases worldwide. Since the same month, there was an obvious increase in the number and capability of DDoS attacks, as demonstrated in Germany, where the number of attacks changed with that of newly confirmed COVID-19 cases.

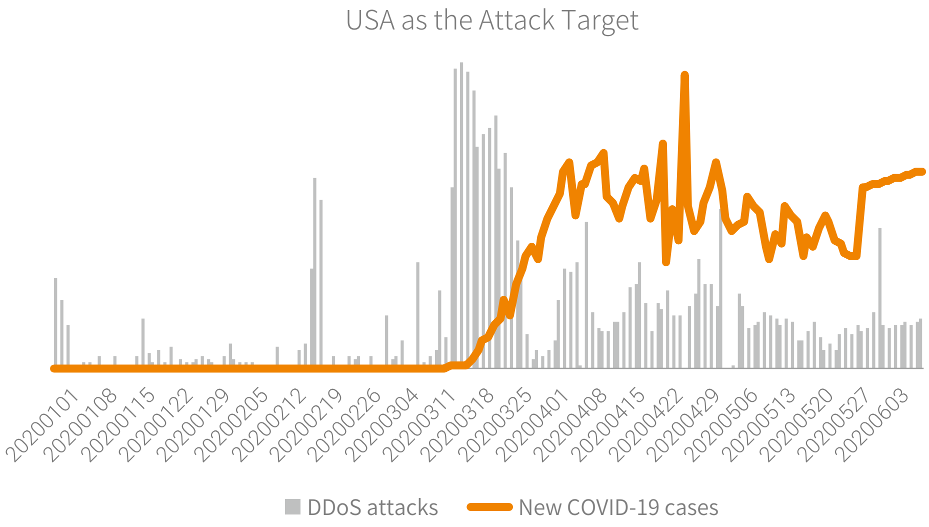

Global DDoS and COVID-19


Germany as the Attack Target

As for the U.S., the pandemic began to erupt in early March accompanied by an increasing number of DDoS attacks in the country but with less attack traffic. Multiple news reports indicated that such harassing DDoS attacks were probably for preventing the news about the COVID-19 pandemic outbreak in the U.S. from spreading in the network.

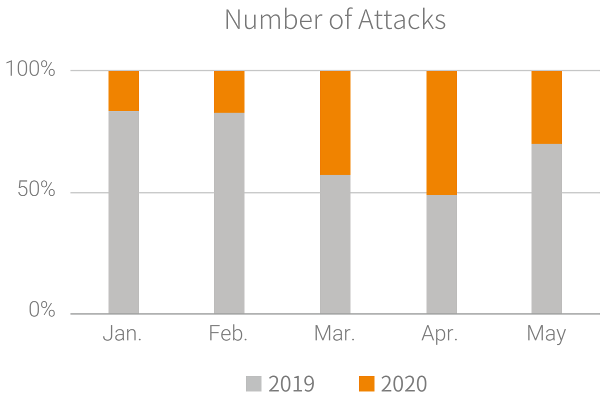
News:

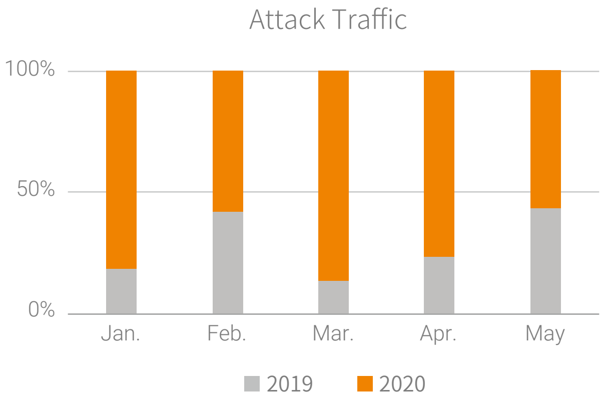
1. The US President Trump declared on March 13 that the country entered a state of national emergency due to the COVID-19 pandemic. At present, the country has more than 1700 confirmed cases and 40 deaths.
2. News from BleepingComputer on March 16, "The United States Health and Human Services Department's web site was hit with a DDoS cyber attack Sunday night and it went offline in the middle of the Coronavirus outbreak."
3. ABC News on March 17, "The distinction is important because there was no apparent breach of the HHS system, which could interfere with critical functions of the lead agency responding to the coronavirus contagion. A DDOS effort enlists automated users -- called bots -- to overwhelm a public-facing system in order to slow it down or even paralyze it." "Nevertheless, the concern is that foreign actors might attempt to exploit the COVID-19 crisis to achieve some of their anti-American goals."


USA as the Attack Target

Attack lethality: Compared with the first half of 2019, the first half of 2020 experienced a decline in the number of attacks with climbing lethality.

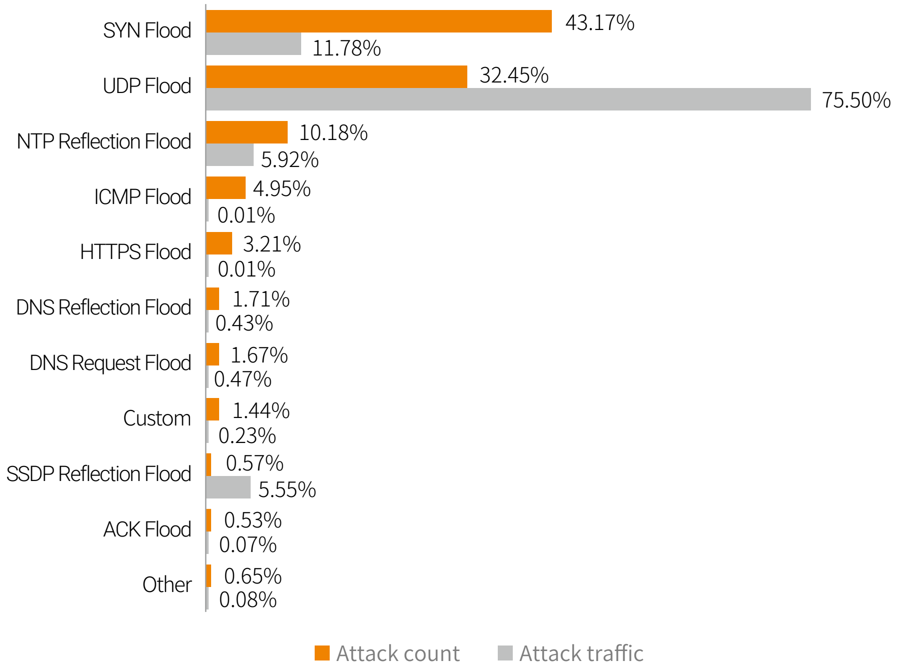
From January to May 2020, except in April when the number of DDoS attacks was on a par with that a year earlier, the other months experienced a year-on-year decrease in the number. However, attack traffic in each month in the first half of 2020 increased year on year.


Number of Attacks


Attack Traffic

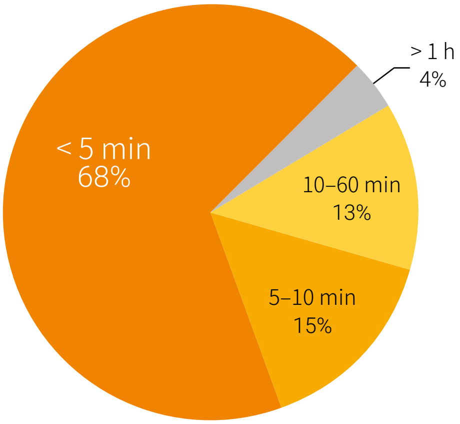
Attack types: SYN flood and UDP flood remained dominant DDoS attacks.

Major attacks in the first half of 2020 were SYN flood, accounting for 43.17% of the total number of attacks. In terms of traffic, UDP floods took the first place, generating 75.5% of attack traffic.



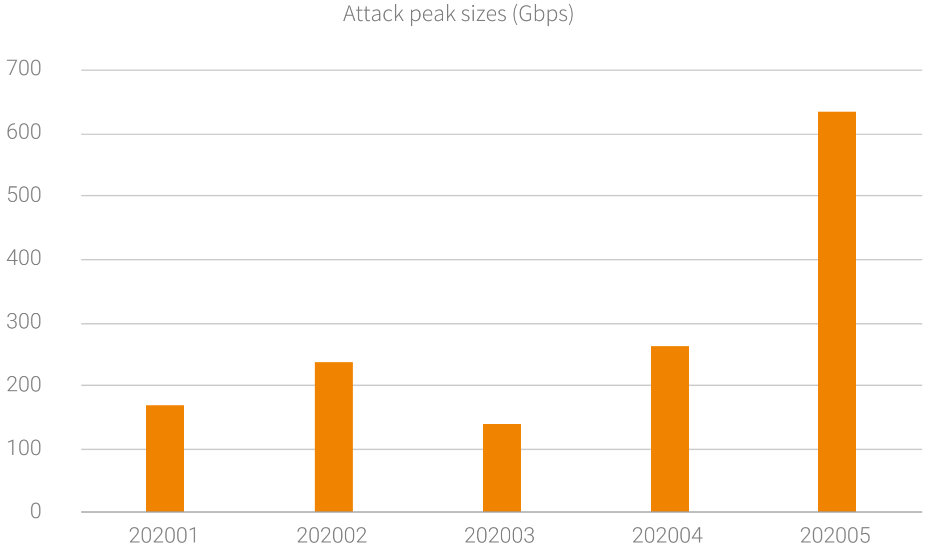
Attack duration: Short-duration and effective attacks were the norm, with 68% of the attacks lasting less than 5 minutes.

68% of the attacks lasted less than 5 minutes. The high proportion of short attacks signals that attackers are attaching more and more importance to the attack cost and efficiency and are more inclined to overwhelm the target service with flood of traffic in a short time, getting users offline and causing high latency and jitters.



Attack peak: May was exposed to the strongest attack, with the peak reaching 634.6 Gbps.

At 17:00 of May 20, NSFOCUS SOC detected an abnormal traffic alert in the global monitoring center, the IP addresses of a customer from Hong Kong were under attack and the maximum attack peak reached 634.6 Gbps. This had been the largest of all attacks targeting NSFOCUS's customers by the time this report was written. According to IP gang intelligence from the NSFOCUS Threat Intelligence ("NTI"), large quantities of source IP addresses involved in the attack were controlled by the IP gang IPGang01 we have continuously monitored. We will elaborate on it in the following "attack gangs" chapter.

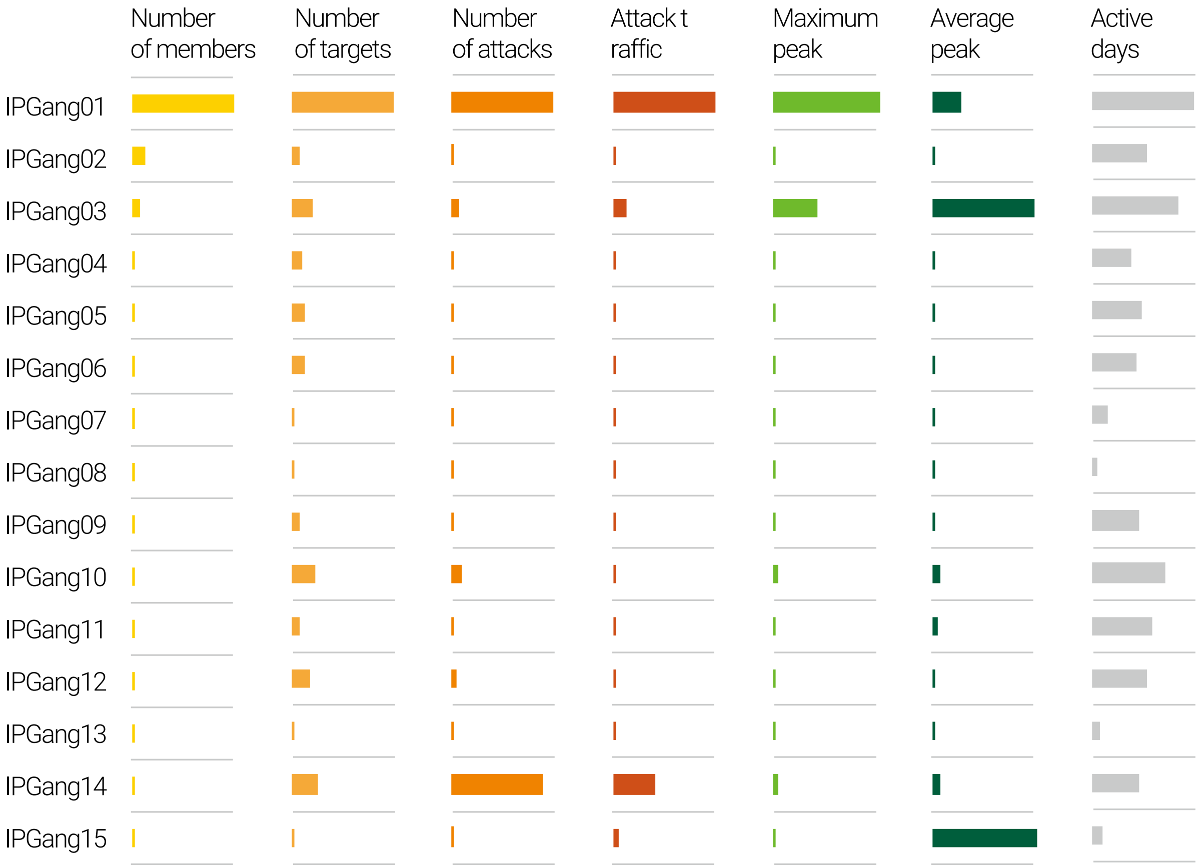


8

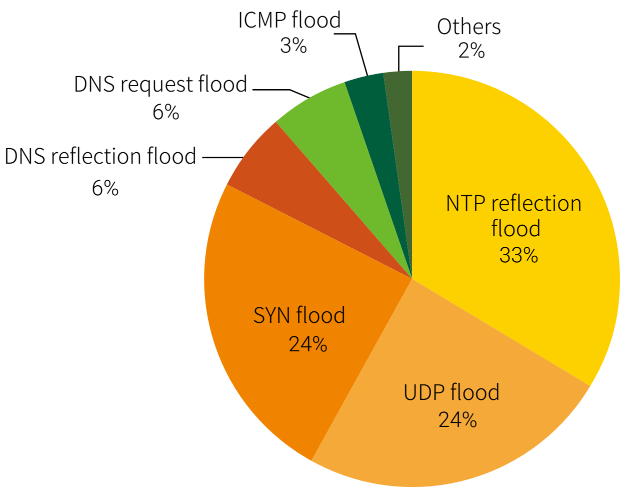
Attack gangs: Among the 15 IP gangs under our continuous monitoring in 2020, the largest contained 217,000 attack sources.

Gang attacks refer to the large-scale attacks with high similarity in attack resources, attack techniques and attack goals. Unlike common attack events initiated by individual attackers, gang attacks usually pursue economic profit or information breach. Gang analysis can offer significant insight into DDoS events and help us take actions in advance.

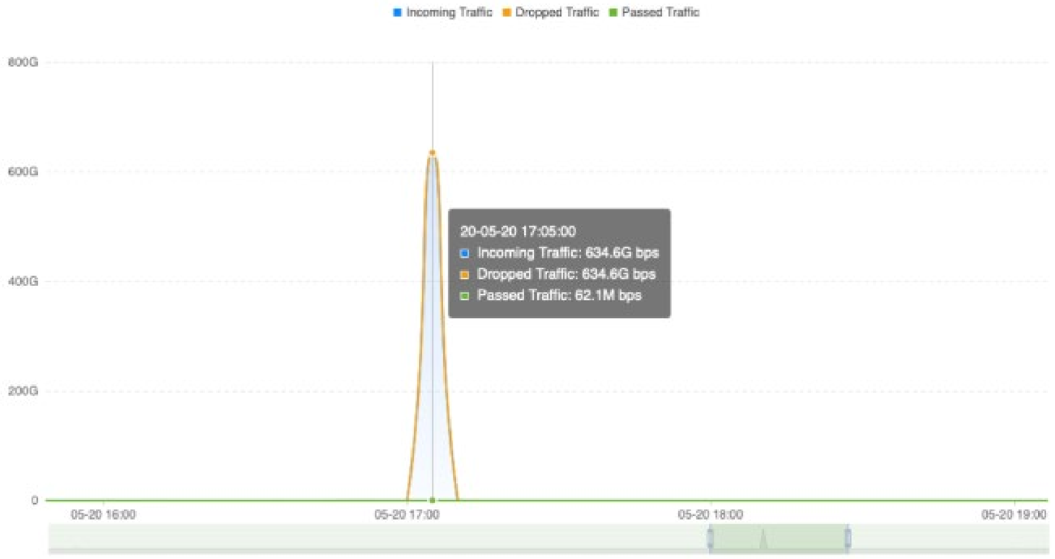
In the first half of 2020, we monitored 15 IP gangs. Comparison of the features of various gangs is shown in the following figure, which is arranged in reverse order of the number of members from top to bottom. A typical example is IPGang01, which was described in detail in the following part.



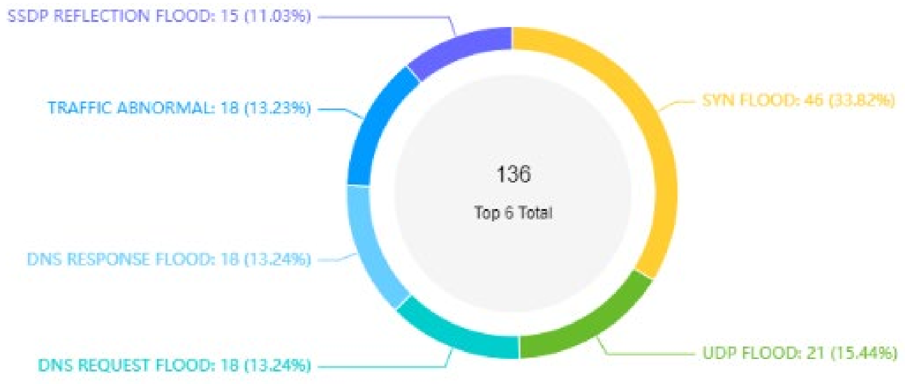
As the largest gang within our monitoring scope, IPGang01 contains 217,000 attack sources and As the largest gang within our monitoring scope, IPGang01 contains 217,000 attack sources and 130,000 monthly active resources. Active days in the first half of 2020 amounted to 164 days. During this period, 58,000 attacks were launched against 1366 targets, generating 13,000 Tb of traffic in total. Distribution of attack features is shown in the following chart.



In March, the gang was the most active and launched 60% of the attack events. In May, attack lethality was the strongest. The above-mentioned attack with the maximum peak of 636 Gbps on May 20 was initiated by the gang. In this attack, SYN floods contributed 33.82% of traffic.



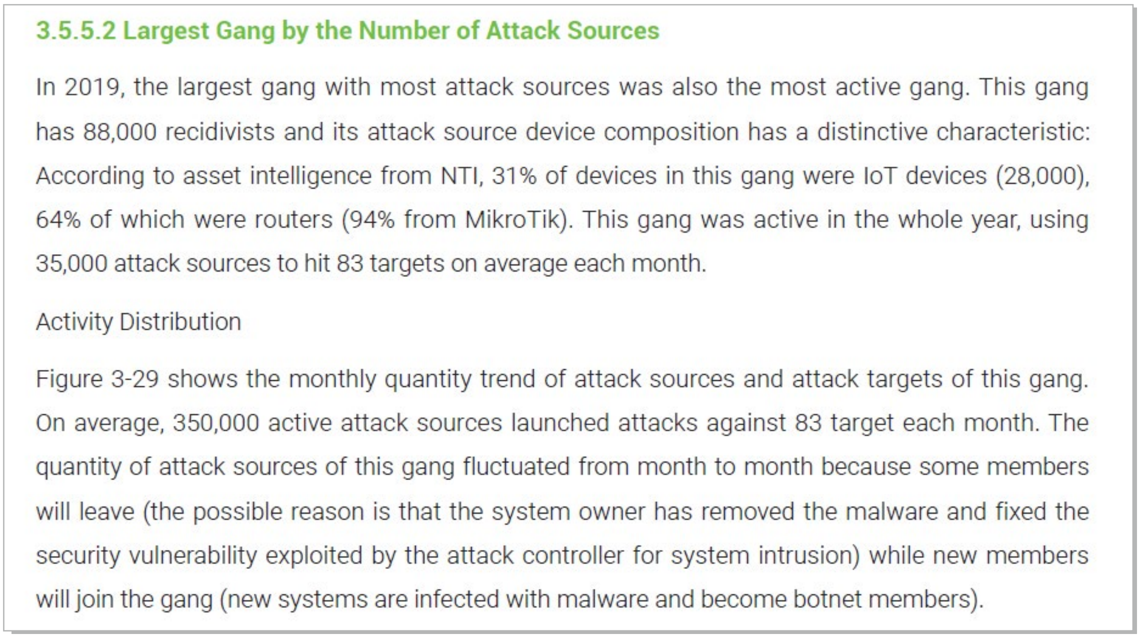
Attack Trend Chart



Attack Types

Note: At 17:00 of May 20, NSFOCUS SOC detected an abnormal traffic alert in the global monitoring center, which indicated that the IP addresses of a customer from Hong Kong were under attack.

In fact, NSFOCUS NSFOCUS Security Lab found the active trace of the gang as early as 2019. In its most active month, the gang had 147,000 attack sources. Its attack members were distributed in various countries, with Russia (27,618), China (22,516) and the USA (17,437) ranking as top three.



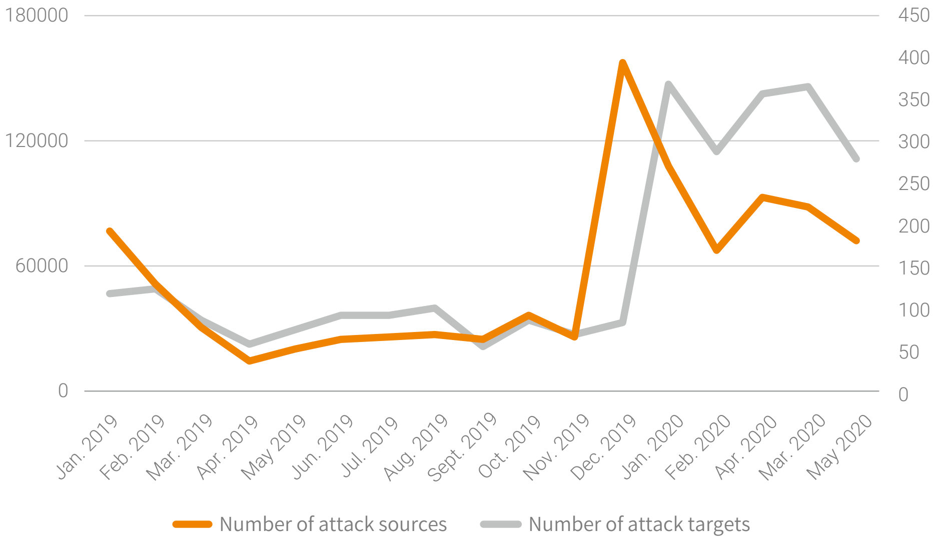
3.5.5.2 Largest Gang by the Number of Attack Sources

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

Activity Distribution

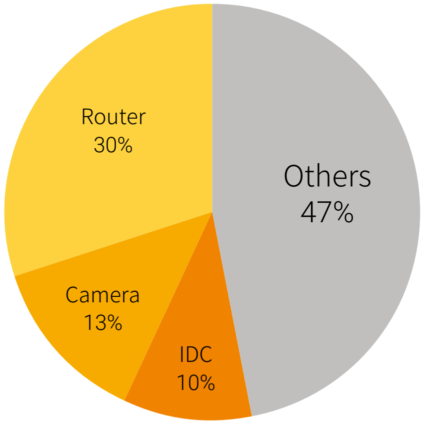
Figure 3-29 shows the monthly quantity trend of attack sources and attack targets of this gang. On average, 350,000 active attack sources launched attacks against 83 target each month. The quantity of attack sources of this gang fluctuated from month to month because some members will leave (the possible reason is that the system owner has removed the malware and fixed the security vulnerability exploited by the attack controller for system intrusion) while new members will join the gang (new systems are infected with malware and become botnet members).

Note: The preceding figure is a description of IPGang01 in NSFOCUS's *2019 DDoS Attack Landscape Report*.

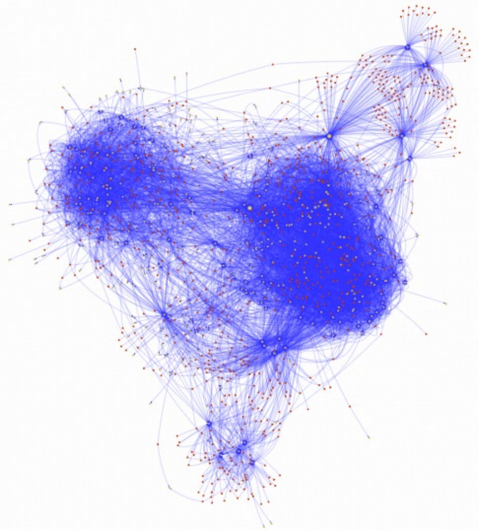


Note: The preceding figure shows the monthly distribution of IPGang01 attack sources and attack targets. The magnitude may differ, because only core gang members (recidivists) were included in statistics from January to November 2019.

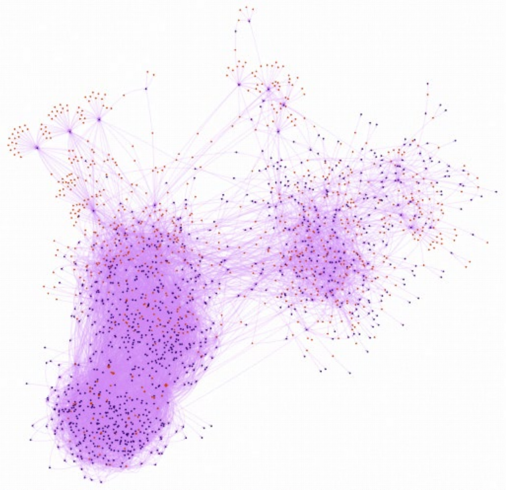
According to NTI's intelligence on assets, routers, cameras, and IDCs accounted for 30%, 13%, and 10% respectively of the attack sources used by the gang.



The following figure is the network map of the relationship between the attack sources and the attack targets of the gang. Red points symbolize the attack sources, and yellow points symbolize the attack targets. Blue lines connect red and yellow points, indicating that the attack sources have launched attacks against the attack targets. The more and the denser the lines are, the closer the relationship between gang members is.



The following figure is the network map of the relationship between the attack sources and the attack events of the gang. Red points symbolize the attack sources, and blue points symbolize the attack events. Purple lines connect red and purple points, indicating that the attack sources have engaged in a certain attack event. The more and the denser the lines are, the closer the relationship between gang members is. It can be seen from the figure that gang members usually engage in the same attack event for large-scale campaigns.



NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com