2020
DDoS Attack Landscape

NSFOCUS

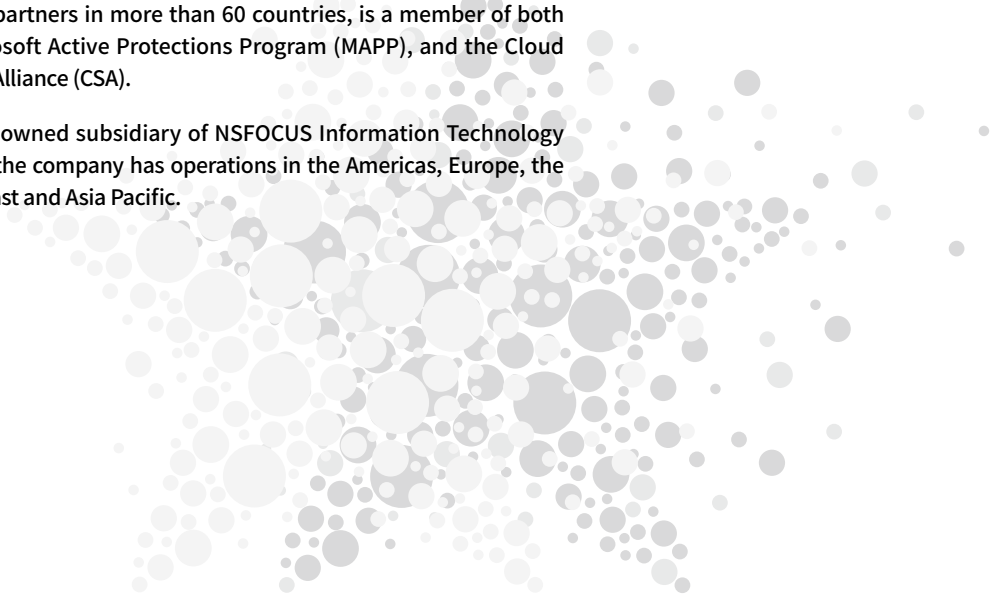
NSFOCUS

About NSFOCUS

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

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

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



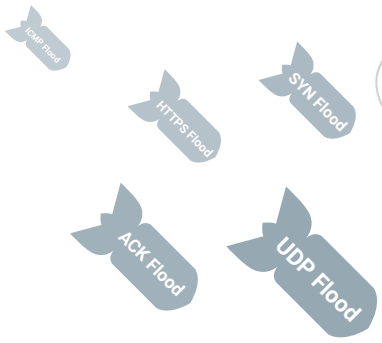
Special Statement

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

CONTENTS

1

Executive Summary

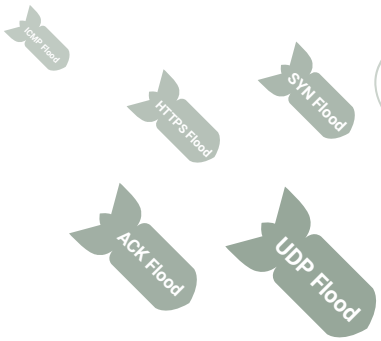


In 2020, the total number[1] of distributed denial-of-service (DDoS) attacks declined a little compared with 2019, probably attributable to effective governance and enhanced protection capabilities of Anti-DDoS products. Despite this, DDoS attacks intensified during the COVID-19 pandemic, especially for healthcare, government, and education sectors. January to April 2020 was a period when China was most severely hit by the pandemic and also a period when this country was most frequently targeted by DDoS attacks, mainly initiated by threat actors from countries outside China. The introduction of 5G networks enables great improvement in speed, capacity and latency. However, it also increased the bandwidth available for larger DDoS attacks. Small-sized DDoS attacks are no longer the mainstream. With the gradual adoption of HTTP 2.0, more and more vulnerabilities in this protocol have been disclosed, giving rise to new threats. While the percentages increased in the numbers of DDoS reflection attacks and reflectors, new types of reflection attacks emerged constantly. In terms of attack source IP addresses, China came in first with the most controlled attack sources. Over 20 million of a Chinese brand mobile phone were reduced to zombies, becoming accomplices of attackers. Compared with the previous year, more Internet of things (IoT) devices have been used in DDoS attacks because for attackers they are cost-efficient, easy to gain control, installed everywhere and increasing day by day.

1 *All data in this report sourced from DamDDoS, NSFOCUS Security Labs, and NSFOCUS Threat Intelligence.*

2

Key Findings



The total number and traffic volume of DDoS attacks declined in 2020.

The bandwidth of DDoS attacks in 5G environment grew steadily. Small and medium-sized attacks overtook small attacks to become the mainstream.

New types of reflection attacks emerged constantly with increasing DDoS reflection attacks and reflectors.

DDoS protection techniques need to evolve with emergence of new attack vectors.

The average attack duration shortened and attack cost continuously declined.

The number of DDoS attacks on healthcare, education, and government sectors increased significantly during the COVID-19 pandemic.

The total traffic volume generated by one IP chain-gang hit 3624 TB, more than doubling the figure of the previous year.

Mirai and Gafgyt were still the most influential Linux/IoT DDoS families across the globe.

The Total Number and Traffic Volume of DDoS Attacks Declined in 2020

As of December 2020, we had detected 152,500 DDoS attacks, which generated 386,500 TB of traffic in total, a year-on-year decrease by 16.16% and 19.67% respectively. This, however, does not mean that we can sit back and take a break. As is known, decreases in the number and traffic volume of attacks are primarily due to anti-DDoS devices' ever enhanced detection and protection capabilities that make their protection prompt and effective, discouraging attackers from pushing ahead, hence the premature end of attacks.

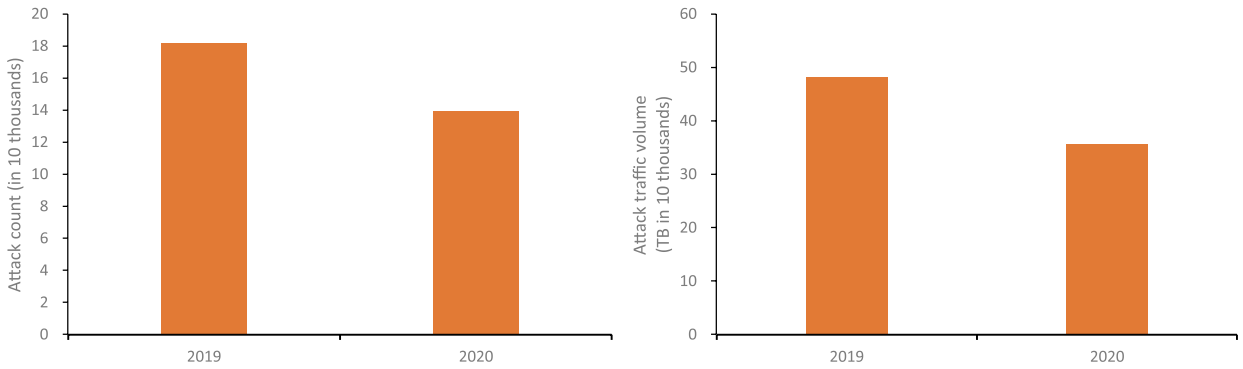


Figure 1. DDoS attack trends in 2020

According to our statistics about the number and traffic volume of DDoS attacks from 2016 to 2020, while 2017 and 2018 were the years when DDoS attacks peaked, 2019 and 2020 were less eventful. But being less eventful does not mean peace in mind. Compared with utter darkness, evening skies illuminated with the shimmering afterglow are more easily to make people lose their way. While the 5G technology is rolling out, IoT devices and mobile devices are increasingly turned into zombies, becoming potential sources of attack traffic. New attack vectors will also be born out of new technologies, such as HTTP 2.0. From the past experience, we can infer that the current decline in DDoS attacks is just temporary and in future there will probably be more DDoS attacks peaking at even higher levels.

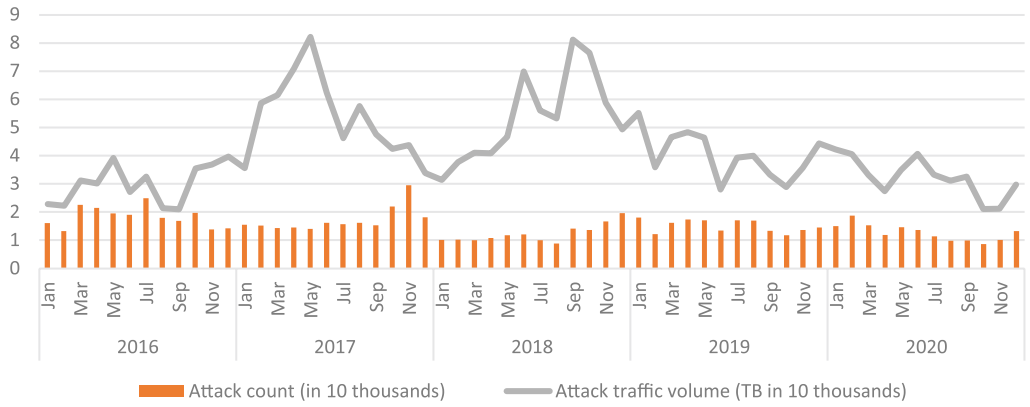


Figure 2. DDoS attack trends in 2016-2020

The Bandwidth of DDoS attacks in 5G Environments Grew Steadily. Small and Medium-sized Attacks Overtook Small Attacks to Become the Mainstream

Over the five-year period from 2016 to 2020, the average peak size of DDoS attacks rose to a new level since the latter half of 2018 despite obvious fluctuations.

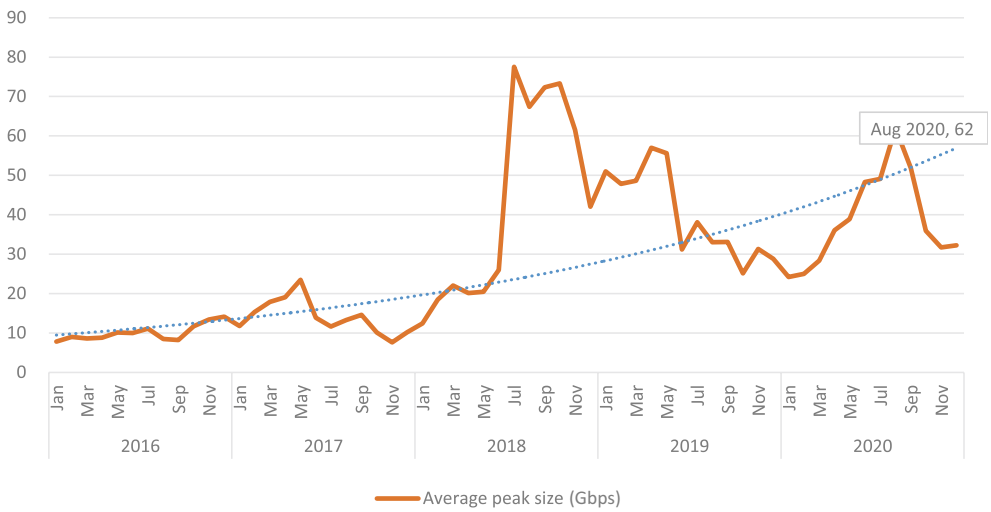


Figure 3. Trend of average peak sizes of DDoS attacks in 2016-2020

Key Findings

Of all DDoS attacks, 18.16% peaked at 5 - 10 Gbps, making up the largest proportion. In 2019, attacks peaking at 1 - 5 Gbps dominated. In 2020, attacks peaking at 5 - 50 Gbps were distributed evenly and accounted for 53.07% of the total DDoS attacks, but the proportion of small attacks peaking below 5 Gbps dropped. It in large part because of using of 5G networks which not only increase the available bandwidth for devices but also bring challenges to DDoS attack protection and mitigation when the benefit is used by attackers to launch DDoS attacks through IoT botnets.

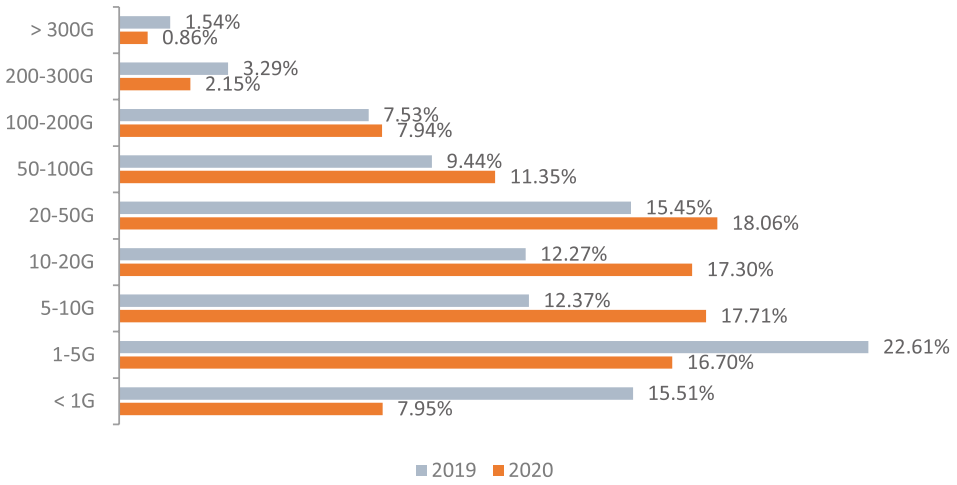


Figure 4. Distribution of attack peak sizes

Seen from quarterly statistics of 2020, small DDoS attacks peaking below 5 Gbps decreased obviously, and attacks whose peak size ranged from 5 - 50 Gbps kept increasing and reached 58.4% in Q4. The proportion and the number of volumetric attacks peaking above 300 Gbps both decreased. By December 2020, there had been 1194 such attacks, 58.97% lower than the figure (2910) in 2019. The proportion also dropped from 1.54% in 2019 to 0.86%. This trend reflects the capacity of ordinary hackers, who are capable of launching low-volume attacks that are difficult to protect against, but are incapable of launching high-volume attacks, which require sophisticated skills.

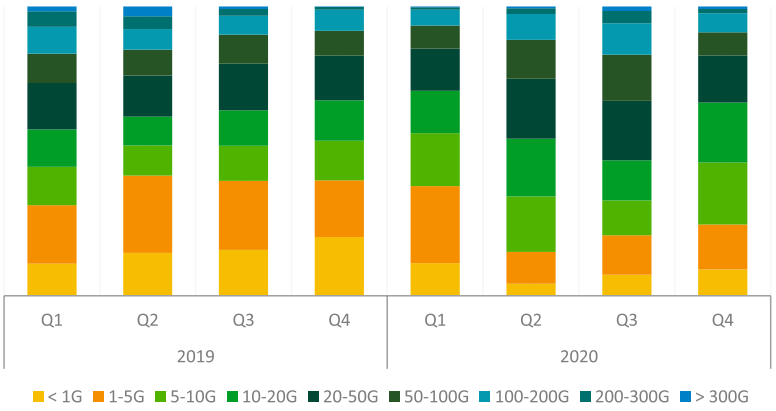


Figure 5. Quarterly proportions of DDoS attacks in 2019 and 2020

New Types of Reflection Attacks Emerged Constantly with Increasing DDoS Reflection Attacks and Reflectors

In 2020, reflection attacks made up 34% of all DDoS attacks. Compared with 2019, the number of reflection attacks increased significantly, and so did the proportion. In this year, NTP (Network Time Protocol) reflection, DNS (Domain Name System) reflection, and SSDP (Simple Service Discovery Protocol) reflection attacks stood out among all reflection attacks. To be more specific, NTP reflection attacks made up the largest proportion in both the number (80%) and traffic volume (53%).

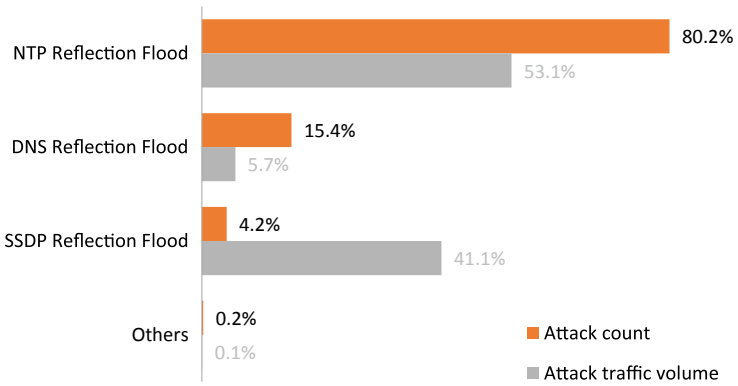


Figure 6. Proportions of reflection attacks and traffic volume

Key Findings

From the attack source type, the proportion of reflectors increased to 14%. Most reflectors are IoT devices. With the fast growth of the 5G technology and IoT, more and more IoT devices are connecting to the network at a faster speed. In contrast to conventional volumetric attack traffic from single IP address, the low-and-slow attack is on the rise by leveraging a wealth of IoT devices. In such attacks, the frequency of packets from each IP address imitate that of packets from legitimate users to evade protection policies that are based on geolocations and rate limiting. To mitigate these attacks, multidimensional detection algorithms have to be used to distinguish between attack sources and normal users.

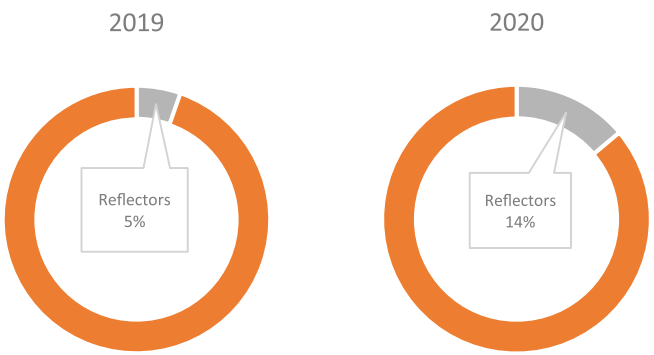


Figure 7. Proportions of reflectors in 2019 and 2020

In February 2020, Amazon Web Services (AWS) said that it suffered a massive DDoS attack of 2.3 Tbps, in contrast to the previous record of 1.7 Tbps in 2018. Through CLDAP (Connection-less Lightweight Directory Access Protocol) reflection, this attack on AWS lasted three days.

In October 2020, Google revealed that, as early as three years ago (2017), it was targeted by a DDoS attack of 2.54 Tbps, which changed the previously perceived record of 1.7 Tbps. This attack also exploited CLDAP, DNS, and SMTP (Simple Mail Transfer Protocol) servers on the Internet to reflect traffic. Data shows that reflection attacks are still dominant in bandwidth consumed DDoS attacks and participated in a lot of renowned volumetric DDoS attacks.

Today, reflection attacks are still changing and evolving, from the first NTP and SSDP attacks to TCP reflection and Memcached erupted in the last two years. Reflection attacks are not difficult to defend

against. But just as attack tactics get better, so must defense strategies. As for mitigation devices, NSFOCUS Anti-DDoS System (ADS) is a good choice as it can effectively detect and protect against various known and unknown reflection attacks.

DDoS Protection Techniques Need to Continue to Evolve with Emergence of New Attack Vectors

NXNSAttack, a new vulnerability in DNS, can be exploited to launch massive DDoS attacks

In May 2020, Israeli researchers reported a new DNS server vulnerability and dubbed it NXNSAttack. This vulnerability exists in DNS's recursive resolution process. Unlike other DDoS attacks that directly target hosts or services, NXNSAttack targets victims' domain name resolution capabilities. It exploits DNS recursive resolvers to initiate DNS lookup requests to a malicious DNS server, which returns crafted responses, resulting in DNS recursive resolvers sending a large number of requests to the victim DNS server. This can achieve the amplification factor of 1620, making the DNS server stop responding, that is, deny service to legitimate users. After the DNS server is attacked, new clients cannot find IP addresses connecting to the service and so cannot know the host names. Compared with common attacks targeting random domain names, this new type of attacks can leverage fewer resources to achieve the same effect while hiding their traces, making it impossible to obtain attack signatures from the composition of domain names.

RangeAmp attacks

In May 2020, researchers from China discovered a new type of DDoS amplification attacks, namely RangeAmp, which exploits the Range field in the HTTP header to initiate malicious requests. By amplifying traffic between content delivery networks (CDNs) or between CDN and the target server by thousands or even tens of thousands of times, RangeAmp will finally exhaust the bandwidth. Such exploit attacks cannot be mitigated with traditional protection algorithms (such as 302 redirect). Keyword-based policies can be used, but require continuous packet capturing, which often lags far behind the attack process. NSFOCUS ADS provides smart protection, which can automatically learn normal traffic's patterns and extract attack fingerprints, enabling the device to generate policies against

unknown abnormal traffic and automatically block attack traffic.

Alarm sounded for HTTP 2.0 DDoS attacks and CC 2.0 era around the corner

Execution of DDoS attacks relies on network protocols. The more widely network protocols are adopted, the more vulnerable networks are. Each layer of network protocols means an attack surface for DDoS attacks. The more complicated a network protocol is, the more diversified potential DDoS attack methods are. With the gradual adoption of HTTP 2.0 comes new HTTP attack threats. Since the protocol's initial application, a slew of vulnerabilities have been reported. More and more studies have found that, different from previous CC attacks, new CC attacks and low-and-slow attacks based on HTTP 2.0 are more devastating, with the potential of degrading server performance more effectively. Besides, HTTP 2.0 makes new attack approaches possible, for example, flood and low-and-slow attacks based on control frames and HTTP 2.0 header compression attacks, as demonstrated by a number of Common Vulnerabilities and Exposures (CVE) records. HTTP 2.0 attacks diversify in form, so simple protection solutions usually cannot work to a satisfactory effect. To address this problem, a multi-layer protection solution should be put in place.

To cope with these new types of attacks, DDoS attack researchers and mitigation operators should continually develop and improve their knowledge and skills so as to work out effective techniques and policies.

The Average Attack Duration Shortened and Attack Cost Continuously Declined

In 2020, the average duration of DDoS attacks registered 42 minutes, a 21% decrease from 2019. We noticed that the longest DDoS attack in 2020 lasted around 13 days, far longer than attacks detected in previous years.

In 2020, DDoS attacks lasting less than 30 minutes accounted for 80%, up 5 percentage points from the previous year (75%). The high proportion of short attacks signals that attackers are attaching more and more importance to the attack cost and efficiency and are more inclined to overwhelm the target service with floods of traffic in a short time, getting users offline and causing high latency and jitters. In

addition, Botnet-as-a-Service (BaaS) and DDoS-as-a-Service (DDoS) have gained momentum for rapid development, which were also to blame for the prevalence of short attacks. Thanks to their availability, platform users are able to launch massive attacks in a very short time as long as they are willing to pay a certain amount of money for a whole lot of mercenary attack resources[1]. In the long run, repeated burst attacks, which are under effective cost control, will greatly aggravate the quality of target services.

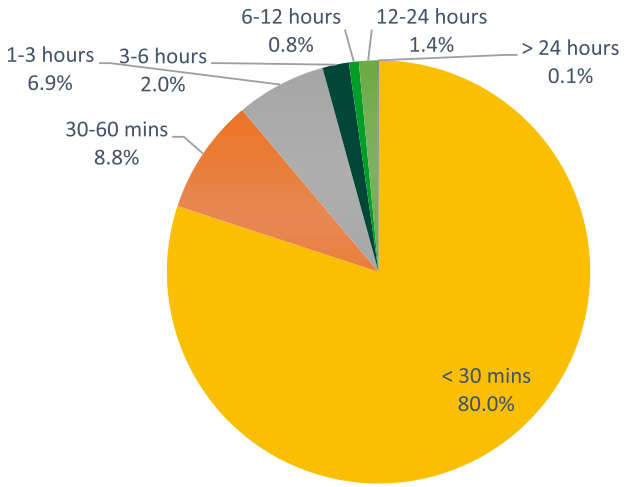


Figure 8. Proportions of attacks by duration

The Number of DDoS Attacks on Healthcare, Education, and Government Sectors Increased Significantly During the COVID-19 Pandemic

The healthcare sector suffered more DDoS attacks during the COVID-19 pandemic than previous years. According to statistics[2], the number of attacks in each month in 2020 H2 increased year on year, with March and April seeing the most attacks. In subsequent months, DDoS attacks trended down. The attack trend after July of 2020 coincided with the same period of 2019, with the monthly number decreasing a bit year on year.

1 *https://nsfocusglobal.com/Gafgy-Botnet-Practitioner-of-the-BaaS-Mode*

2 *https://nsfocusglobal.com/2020-mid-year-ddos-attack-landscape-report/*

Key Findings

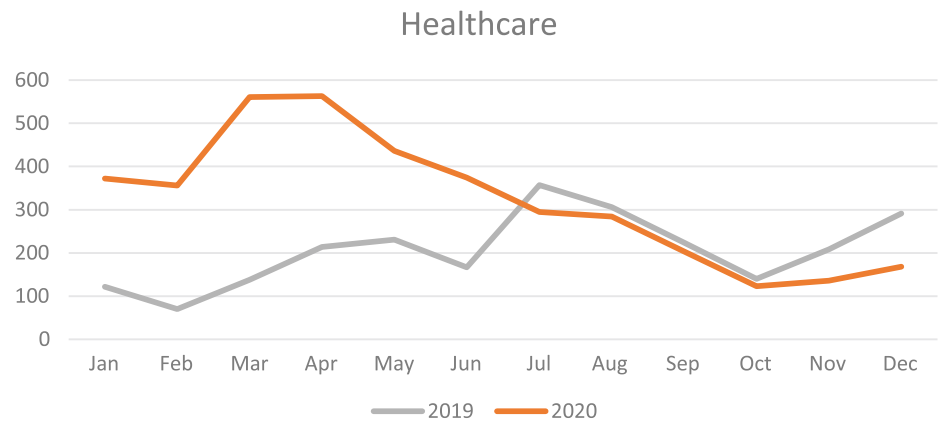


Figure 9. Trend of attacks on the healthcare sector

DDoS attacks on government and education sectors trended similarly. A slight difference is that for these two sectors, DDoS attacks in the latter half of the year declined more rapidly.

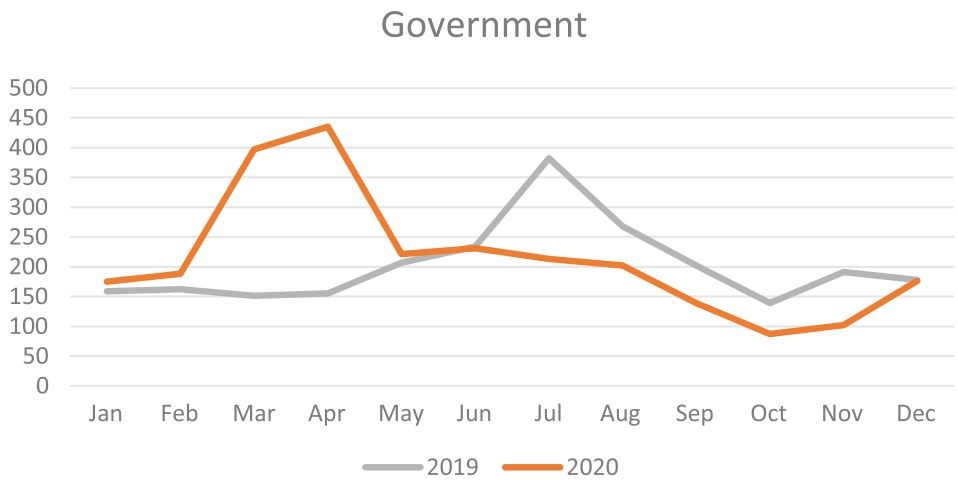


Figure 10. Trend of attacks on the government sector

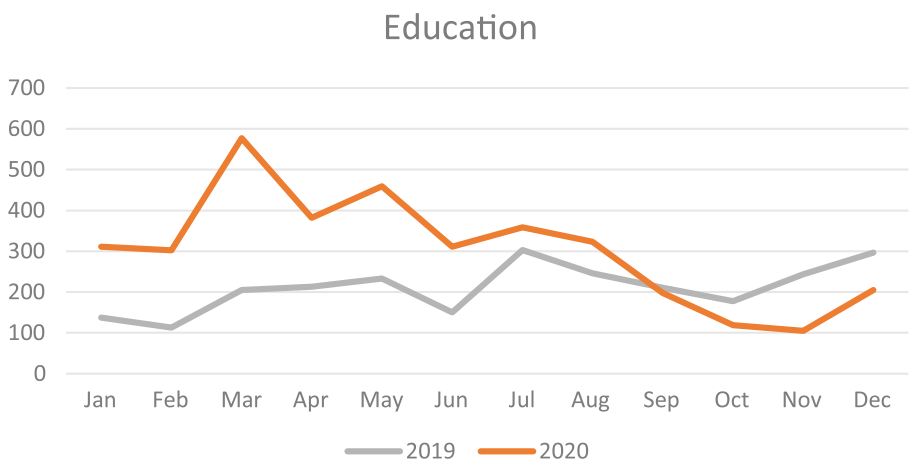


Figure 11. Trend of attacks on the education sector

The Total Traffic Volume Generated by One IP Chain-gang Hit 3624 TB, More Than Doubling the Figure of The Previous Year

A DDoS attack is usually conducted by multiple actors that work in a coordinated manner. Such actors are mostly repeat hackers found to be repeatedly linked with malicious activities. We call these groups "IP chain-gangs". In this report, through analysis of DDoS attack data collected by NSFOCUS in 2020, we have identified multiple IP chain-gangs and done a systematic research on their behavior.

The logic behind this research methodology is that IP addresses with similar historical attack behavior form an IP chain-gang. The behavior similarity is reflected in the following aspects:

- Behavior similarity in a short time: hitting the same target again and again using the same attack method in the same period.
- Behavior similarity in the long run: hitting the same target repeatedly using the same attack method in different periods.

After analyzing behaviors of IP chain-gangs and profiling major gangs, we found that:

1. Infrastructures such as IoT devices and Internet Data Centers comprised a large proportion of those IP chain-gangs being controlled over a long period.
2. The total traffic volume generated by one group hit 3624 TB, more than doubling the figure of the previous year.

Gang Size

In 2020, a total of 45 active gangs were found, most of which had 200 to 10,000 members, as shown in figure below. Besides, four gangs consisted of over 10,000 members and the largest one had 49,000 members.

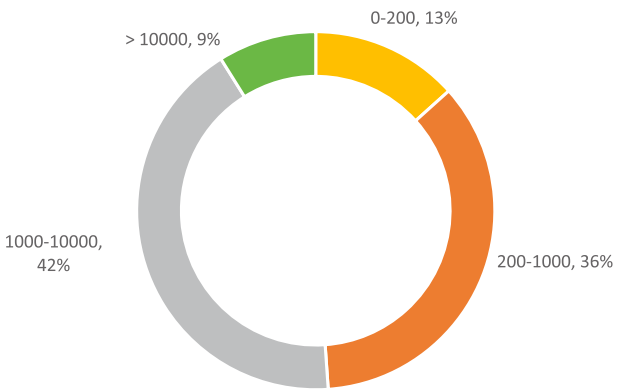


Figure 12. Distribution of IP chain-gangs by size (each section indicates a size range)

Total Traffic Volume

The figure below shows the distribution of IP chain-gangs in terms of traffic generated by all members within a gang. The total traffic volume generated by one gang hit 3624 TB, more than doubling the figure of the previous year.

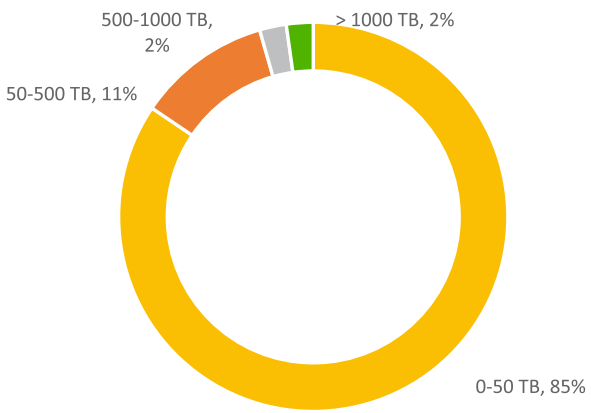


Figure 13. Distribution of IP chain-gangs by total traffic volume

Attack Resource Type

Attack resources that can be long manipulated are mainly IDCs and IoT devices. According to statistics around resource types, IoT devices were the most common type in IP chain-gangs, accounting for 31% of all controlled resources. Specifically, cameras made up the largest proportion (15%), followed by routers (12%) and VoIP (3%).

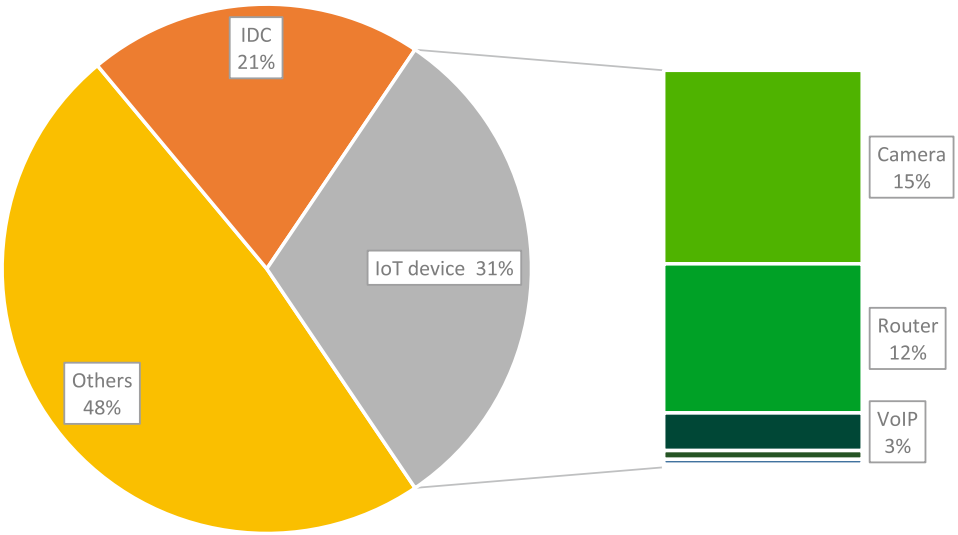


Figure 14. Distribution of resource types of IP chain-gangs

Mirai and Gafgyt Were Still the Most Influential Linux/IoT DDoS Families Across the Globe

Botnet Facts

NSFOCUS Security Labs detected over 1,220,000 instructions generated by DDoS botnets in 2020, nearly doubling the figure in 2019. Of all these instructions, 1,210,000 were for DDoS attacks.

Analyzing data from the dimensions of families (including variants), attack targets, and attack durations, we found that there were over 190,000 attacks across the year, with the most happening in August. The following figure compares the monthly number of DDoS attacks from January to December in 2019 and 2020.

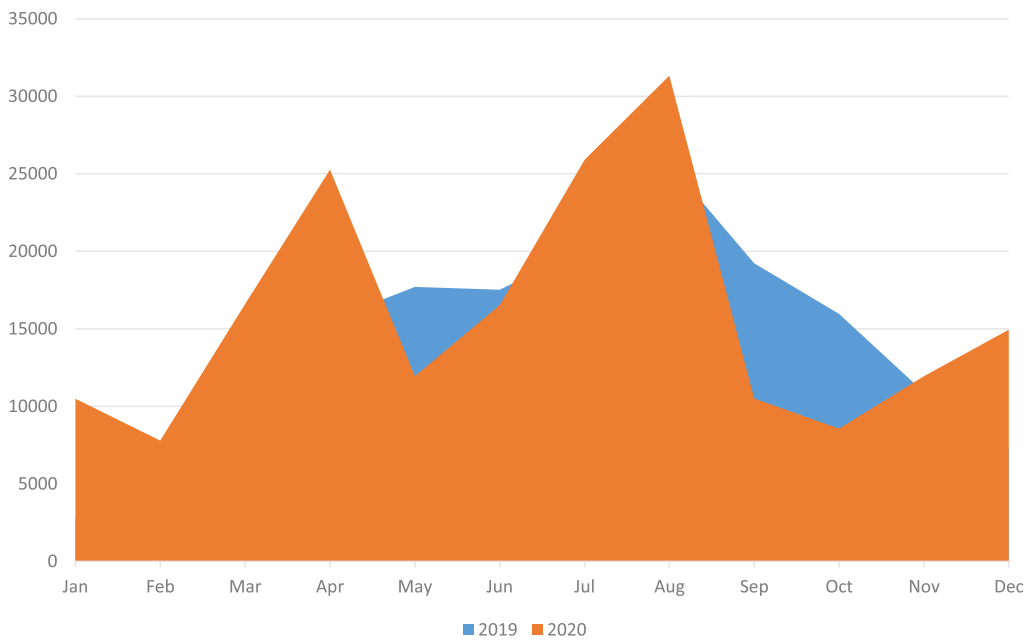


Figure 15. Comparison of the monthly number of DDoS attacks

As for DDoS attack types, TCP flood, UDP flood, and CC attacks were the top three attacks. In particular, the proportions of TCP flood and CC attacks increased a lot from the previous year.

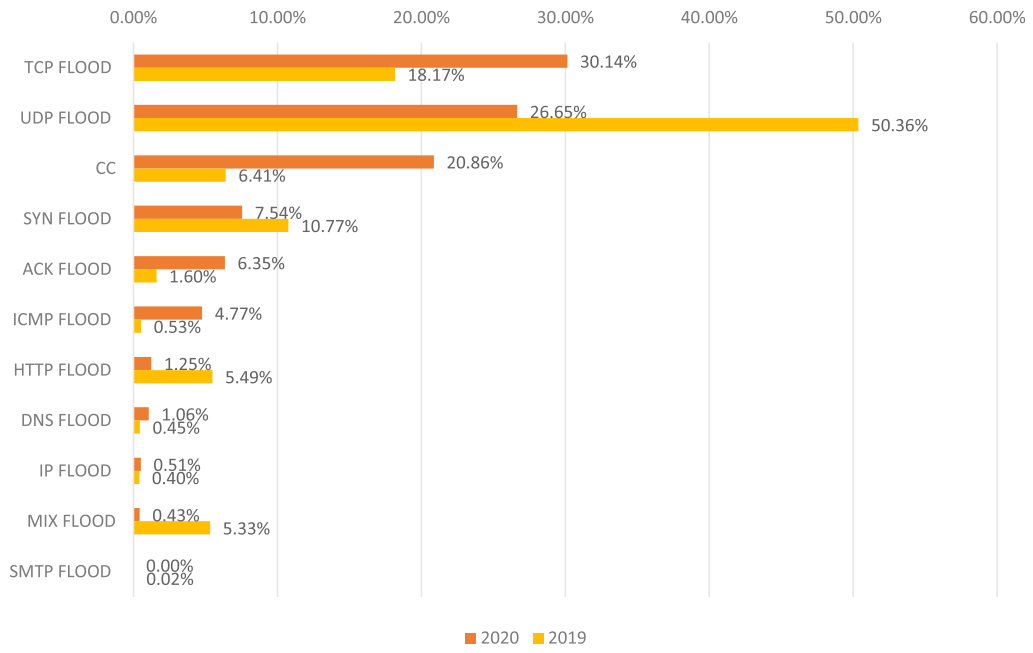


Figure 16. Comparison of DDoS attack types

The 190,000 DDoS attacks were mainly initiated by 10 families. According to NSFOCUS Security Labs' observation, Mirai was the most active family, responsible for three-fourths of attacks.

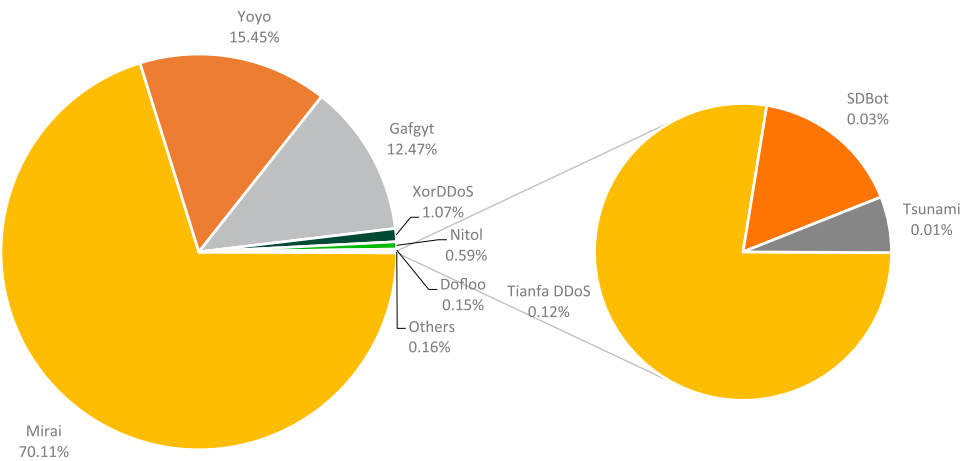


Figure 17. Proportion of attacks initiated by each family

Key Findings

When it comes to the issuance of instructions, things are different. Dofloo (AESDDoS) issued nearly 60% of instructions, while Mirai was linked with less than 20%. Likewise, SDBot, which initiated only a small proportion of attacks, was ranked third in terms of the number of instructions. Such a variance mainly stems from these families' attack patterns and popularity on international black markets.

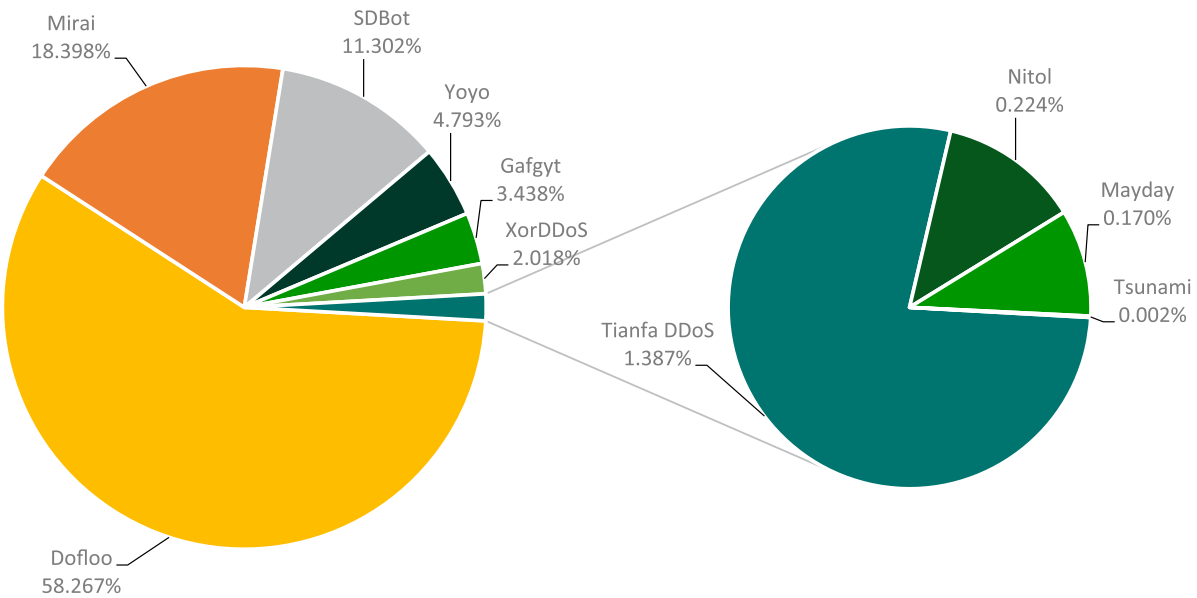


Figure 18. Proportion of instructions linked with each family

In terms of propagation, DDoS families exploited over 130 IoT vulnerabilities in 2020. Payloads used were nothing much different from years past. The top 2 vulnerabilities exploited were still CVE-2017-17215 and CVE-2014-8361. Other types included remote command execution and injection vulnerabilities. Also, Windows-based families spread themselves by using traditional methods like SQL injection, remote exploitation, brute force, and software cracking. The following figure shows most common IoT vulnerabilities exploited by DDoS families in 2020.

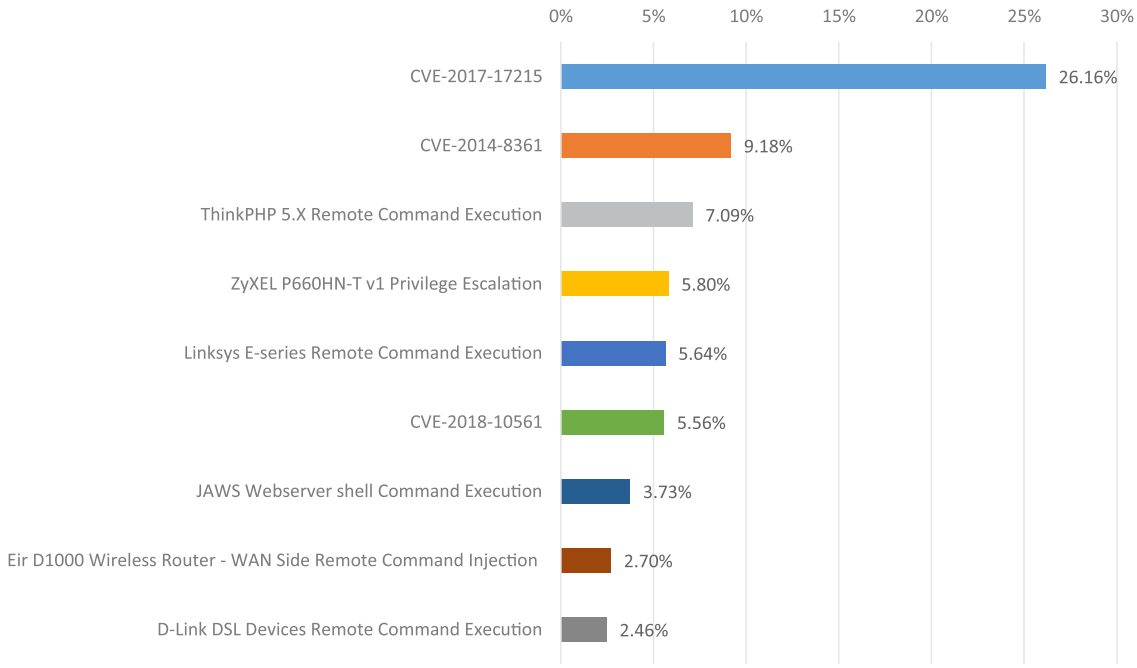


Figure 19. IoT vulnerabilities exploited

Highlight DDoS Families

Mirai and Gafgyt

Mirai and Gafgyt were still the most influential Linux/IoT DDoS families across the globe. These two families have been widely used because of the open-source codes, which gives rise to a large number of variants. Some hackers even developed new families by modifying and improving the codes. All these make Mirai and Gafgyt the biggest threats in IoT environments.

Mirai and Gafgyt have the largest number of command and control (C&C) servers and the largest scope of impact. According to NSFOCUS Security Labs' botnet tracking in 2020, the two families had over 1500 C&C addresses (by November), 94% of which were active. On average, 4 - 5 new C&C servers were deployed each day. These C&C servers attacked more than 220,000 IP addresses/domain names, involving over 700 targets per month. The following figure shows the combined monthly number of IP addresses/domain names attacked by the two families.

Key Findings

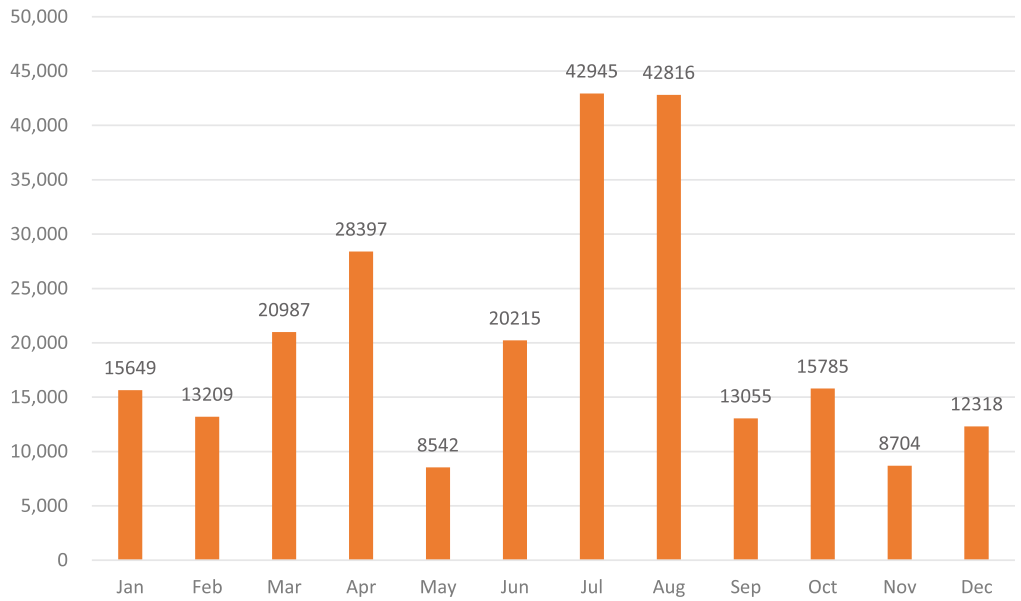


Figure 20. Combined monthly number of IP addresses/domain names attacked by Mirai and Gafgyt

While conducting DDoS attacks, Mirai and Gafgyt resort to a variety of means, including the SYN/ACK flood, IP flood, UDP/TCP flood, DNS flood, Greth flood, and HTTP flood, from the network layer to the transport layer.

For propagation, they most frequently use a vulnerability in Huawei HG532 routers and a remote code execution vulnerability in Realtek rtl81xx SDKs. They are also two most common vulnerabilities exploited by IoT botnets. Besides, a few Trojans use payloads suspected to be 0-day vulnerabilities, indicating that controllers are seeking for more channels for faster propagation.

Last but not least, Mirai and Gafgyt open-sourced their codes, which facilitates development of new DDoS families of similar nature. At the end of 2019, DarkNexus, a DDoS family controlled by the Mirai operator, began to make trouble. Compared with Mirai and Gafgyt, DarkNexus acts in a more complicated pattern, with more novel attack methods and more covert chains of infection. Besides, DarkNexus allows customization of scanning tasks, a new function unavailable in Mirai and Gafgyt, making targeted propagation possible. These characteristics add to the uncertainty of IoT security.

Dofloo, SDBot, and Yoyo

Dofloo (AESDDOS) has long been thought of belonging to the same DDoS family as XorDDoS and Tianfa DDoS. This family mainly serves customers on gray and black markets, targeting gaming and gambling sectors. With 90% of C&C servers and victims in China, Dofloo attacked targets mainly via CC flood, TCP flood, and UDP flood in 2020.

Unlike Mirai and Gafgyt, both of which have global presence, Dofloo has hit only a small number of targets with a limited number of C&C servers in sporadic attacks. This is probably because it is hosted on a small platform. But this does not mean that Dofloo is less active. In 2020, NSFOCUS Security Labs found that Dofloo issued instructions quite frequently at an interval of 5 seconds to 1 minute. We took 10 minutes as the upper limit of the intervals and got the longest duration of 31 hours during which instructions were continuously issued by the same C&C server against the same target. Such a long duration, plus the number or duration of attacks indicated in each instruction, is enough to cripple the target's business.

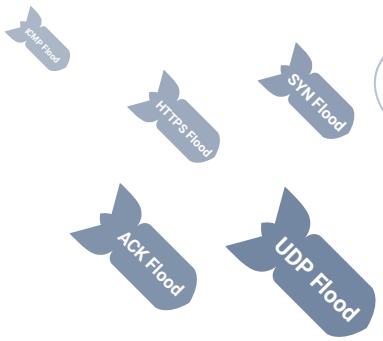
Similar to Dofloo, SDBot has a limited number of C&C servers and targets. In particular periods in 2020 H1, it was especially active, issuing attack instructions at a high frequency over a period as long as 34 hours. The attack method it mainly used was TCP floods.

The Yoyo family has been active for more than a decade in the DDoS field. According to our observation in 2020, this family had a very small number of C&C servers, operating in a scope smaller than Dofloo. Still, it could be very active in particular periods and such a high level of activity could last for months steadily. In the past year, Yoyo mainly used ICMP floods to overwhelm more targets than Dofloo in a wider scope, covering "running points platforms", accelerators, download sites, online video interfaces, gambling, and private game servers.

According to up-to-date data, these families, though small in scale, can get very active after receiving a task and so should never be underestimated. Amid the trend of DDoS trojans evolving towards homogeneity, represented by Mirai and Gafgyt variants, these less prevalent families' existence reflects differences in the cybersecurity ecosystem between countries/regions and provides a perspective into understanding such differences.

3

Conclusion



2020 was a year full of challenges. We were also deeply impressed by one after another fierce battle in the cyberspace between rivals because of the COVID-19 outbreak, ever changing international relations, and unbalanced development of 5G technologies. International events are good chances for hackers to launch cyberattacks and various novel attack vectors merge from time to time. With the fast development of 5G technologies and more IoT devices connecting to the network, hackers begin to launch low-and-slow attacks leveraging massive IoT devices. Such attacks call for new defenses. Mobile devices constantly end up accomplices of malicious actors, posing a huge challenge to traditional DDoS protection techniques and architectures. Reflection attacks are still a dominant type of DDoS attacks, with new types coming constantly, urging for adaptive protection methods. Novel attack methods targeting HTTP 2.0 also appear now and then, which requires DDoS protection techniques to change accordingly. To effectively protect against DDoS attacks, we have to make full use of big data and artificial intelligence technologies. Only in doing so, can we keep up with the development of hacking skills and methods amid the fast-changing landscape. By predicting what hackers will do and developing new algorithms, we can know and further defeat the enemy, thereby ultimately winning this cyber war.

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com