DDoS Attack Statistics and Trends Report for 2020

Genie DDoS Security Response Team

DDoS Attack Statistics and Trends Report for 2020

PREFACE

Along with the emergence and advancement of disruptive internet technologies, DDoS (Distributed Denial of Service) attacks are evolving and growing rapidly in scale, frequency, and sophistication. Organizations face potential threats to their network environment that may cause severe impacts to their operations, such as business downtime, data breach, or even ransom demands from hackers.

Led by the global pandemic, the year 2020 witnessed a major boom in the stay-at-home economy, and consequently, the amount of DDoS activities which rose to an all time high. Protecting against DDoS threats is no longer a new subject, but rather an issue that should be closely regarded by any modern organization.

As a leader in network traffic analysis and DDoS protection of the APAC region, Genie Networks has been constantly focused on the telecom and internet service provider sector. These carrier-grade networks are not only greater in scale and complexity compared to regular enterprise networks, but also require a defense mechanism with higher standard and performance. Genie Networks provides just the right solution for these customers. Over the past twenty years, we have helped numerous Tier-1 telecom service providers secure against DDoS threats.

This analysis report uncovers the 2020 DDoS statistics of several Tier-1 telecom service provider networks in the APAC region, including those of Internet service providers, data center/co-location providers, and mobile operators. As Genie Networks specializes in L3 and L4 volumetric attack detection, this report will thus focus on volumetric DDoS attack analysis - in terms of quantitative statistics on the attack vector, trend, scale, duration, and source distribution. We will also discuss a few of the largest volumetric attack cases in 2020.

Unlike many DDoS analysis reports available in the market today, which rely primarily on subjective survey data, this report counts on statistical analysis based on actual attack data to avoid the likelihood of subjective misinformation.

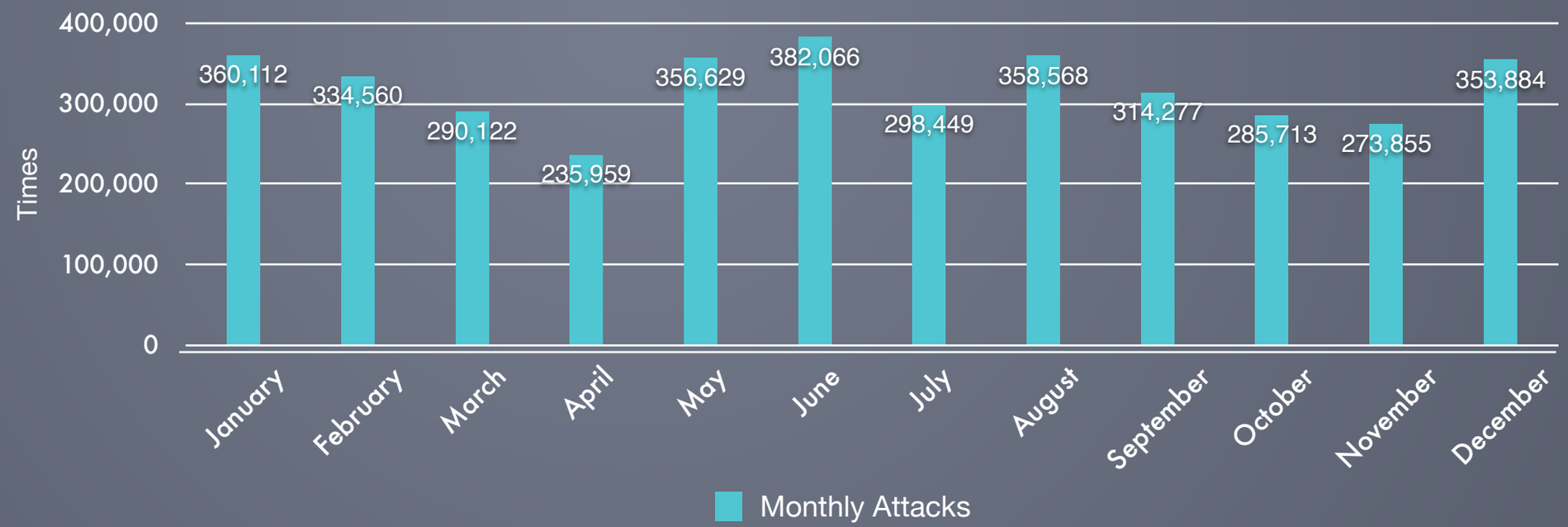
Genie DDoS Security Response Team

ATTACK FREQUENCY | OVERALL TREND

The number of DDoS attacks observed for 2020 falls around 3.7 million times. The number of attacks observed monthly falls between 200,000 to 400,000 times, with the highest at 380,000 times in June, and lowest at 230,000 times in April. The monthly attack frequency fluctuates at a considerable degree, with a growth/decline range (MoM+) between -15% and +40%.

On average, there had been approximately 300,000 attacks every month, which is equivalent to:

- ✓ 10,146 times per day;
- ✓ 423 times per hour;
- ✓ 7 attacks per minute



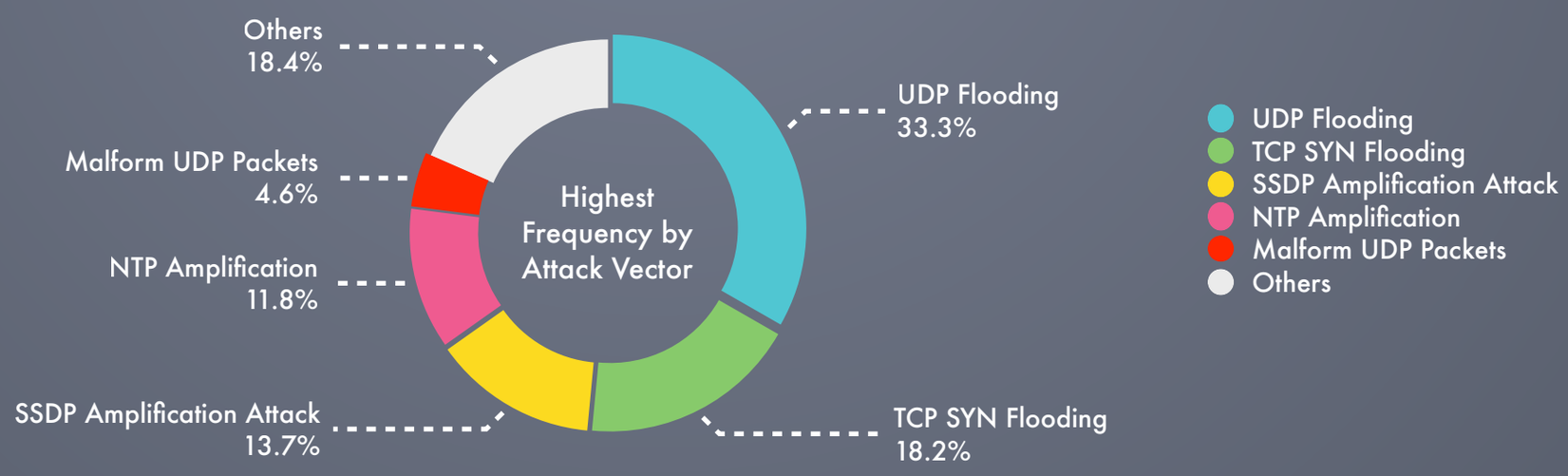
ATTACK FREQUENCY | BY VECTOR

This report covers different types of DDoS attack vectors that can be divided into the following categories: TCP flood attacks (such as SYN Flood, RST Flood, SYN-RST Flood... etc.), UDP flood attacks, protocol misuse attacks (such as Malformed TCP packets, Malformed UDP packets, Land Attack, IP Protocol Null, ICMP abuse... etc.), reflection amplification attacks (such as SSDP Amplification, NTP Amplification, CLDAP Amplification, DNS Amplification...etc.), worm attacks (such as SQL Slammer, Code Red, Sasser... etc.), and application layer flood attacks.

The top 5 DDoS attack vectors for H1 2020 are：

- ✓ 1st, UDP Flood - 33.3%
- ✓ 2nd, TCP SYN Flood - 18.2%
- ✓ 3rd, SSDP reflection amplification - 13.7%
- ✓ 4th, NTP reflection amplification - 11.8%
- ✓ 5th, Malformed UDP packets (port 0) - 4.6%
- ✓ Others - 18.4%

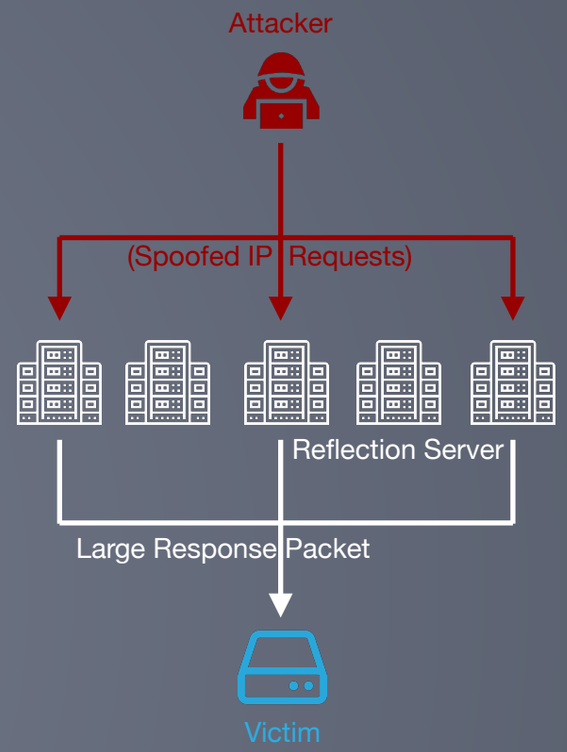
In total, the most common attack vector for 2020 is reflection amplification, then comes UDP Flood and TCP SYN flood.

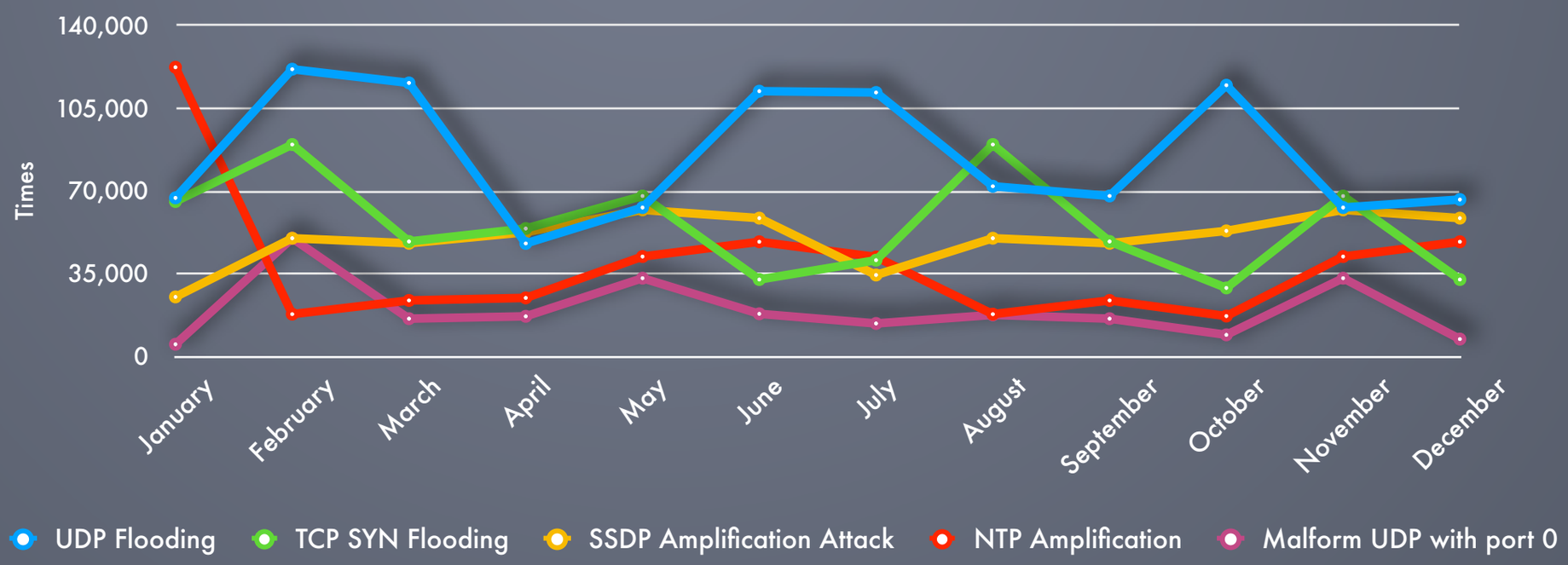


ATTACK FREQUENCY | BY VECTOR TREND

The Top 5 Attack Vectors (by months) for 2020 had not seen much change. Other than TCP RST flood and DNS reflection amplification attacks reaching top-5 for a few months and DNS reflection amplification making the fifth spot for January, the top 5 were usually UDP flood, TCP flood, SSDP reflection amplification, NTP reflection amplification, and Malformed UDP packet attacks.

On another note, the attack traffic generated by the 5th ranked Malformed UDP packets (port 0) is primarily considered a side effect of a reflection amplification attack. This is because during the process of such an attack like SSDP or NTP reflection amplification attacks, the reflection servers usually respond to the attacker's Spoofed IP requests with extremely large UDP packets due to the high amplification factors. These large packets will be fragmented into smaller ones for transmission with a smaller MTU. While only the first IP fragment contains a UDP header, the subsequent fragments would be recognized by the router as UDP packets without UDP headers and source/destination port number equals 0. In summary, an often high-ranked Malformed UDP packet usually indicates a high percentage of reflection amplification attacks.



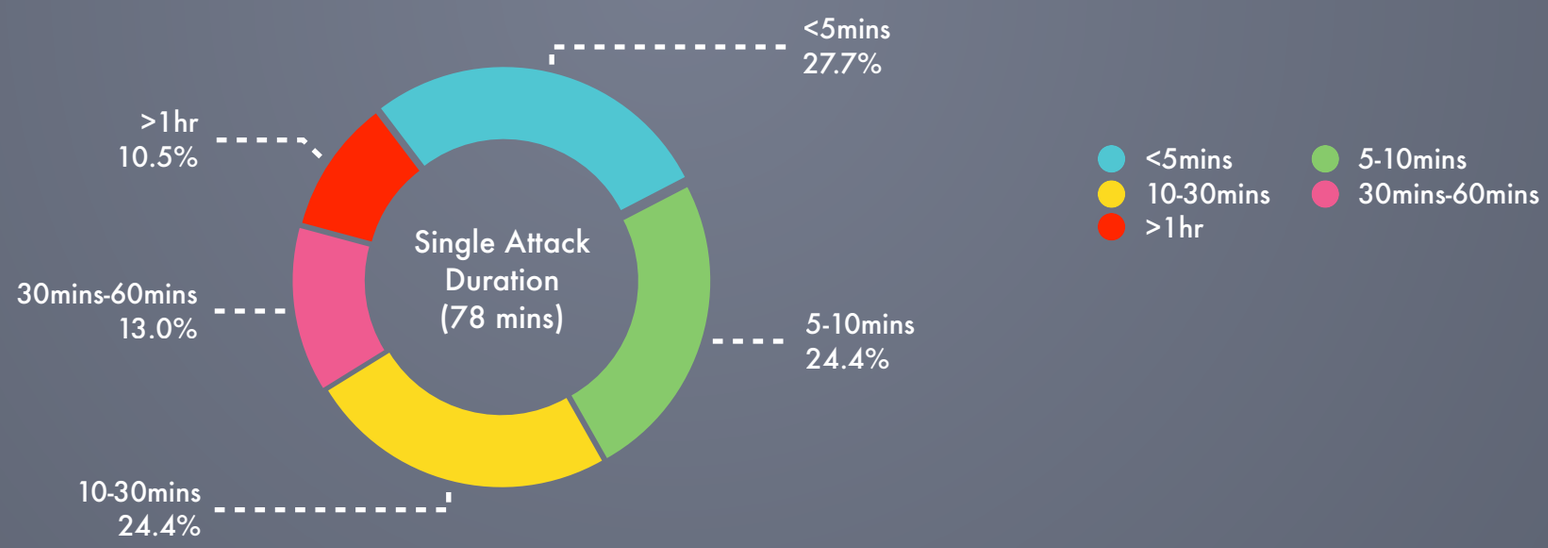


ATTACK FREQUENCY | BY DURATION

The average attack duration recorded for 2020 is about 78 minutes (1.3 hours), with most attacks ending within 5 minutes.

It is observed that more than half of the attacks lasted between 5 to 30 minutes. While attacks that lasted less than 5 minutes accounted for only 8.2% and attacks longer than one hour accounted for only 11%, the overall average attack duration still went up to 1 hour. This is because the number of attacks longer than one hour usually took much more than one hour - some even lasted for several hours or days, bringing up the average duration value significantly.

In addition, a very large percentage of attacks lasted only a few minutes from initializing, producing volumetric attack traffic, till finishing. Therefore, we can conclude that an effective DDoS defense system should have the ability to detect, alert, and mitigate during the initialization stage.

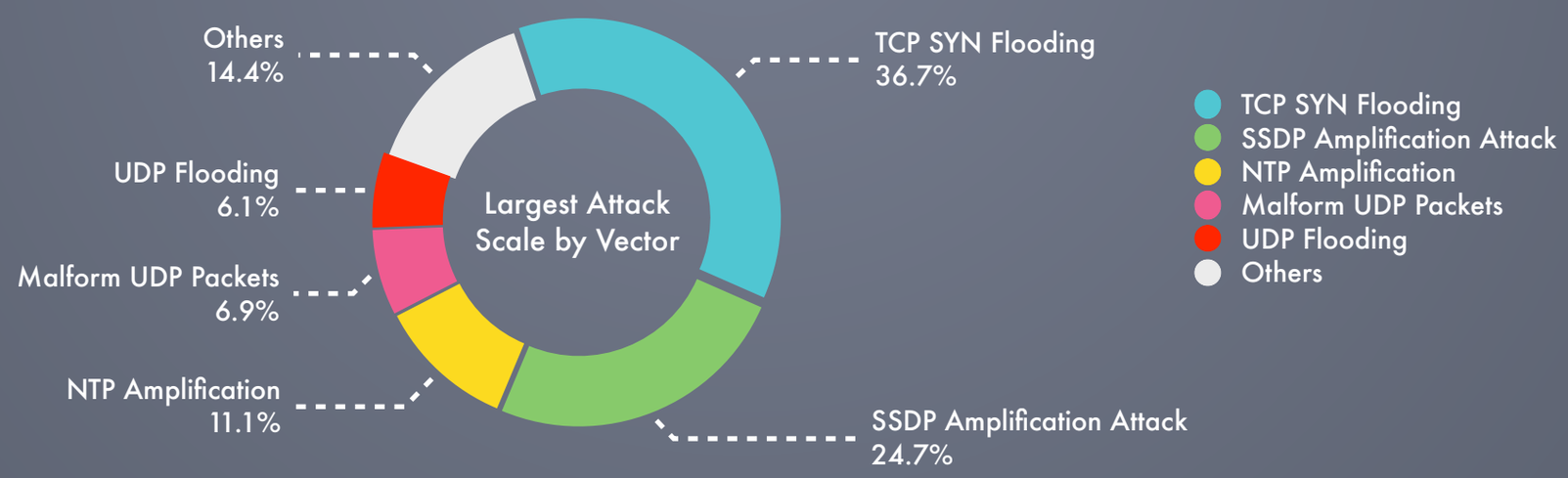


ATTACK SCALE | BY VECTOR

The top five attack vectors of H1 2020 based on attack scale are：

- ✓ 1st, TCP SYN Flood - 36.7%
- ✓ 2nd, SSDP Reflection Amplification - 24.7%
- ✓ 3rd, NTP Reflection Amplification - 11.1%
- ✓ 4th, Malformed UDP Packets (Port 0) - 6.9%
- ✓ 5th, UDP Flood - 6.1%
- ✓ Other attacks in total - 14.4%

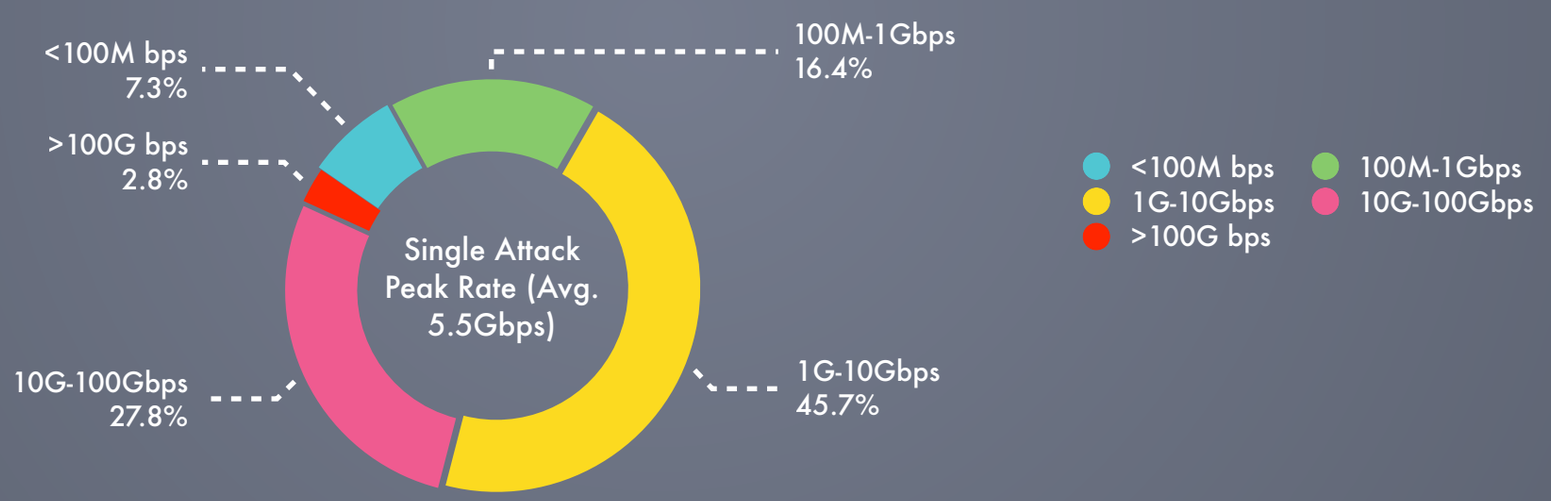
Comparing the top 5 vectors in attack scale with the top 5 vectors in attack frequency, we can observe that due to the scale of a single UDP flooding attack being generally smaller compared to a reflection amplification or TCP SYN flood, despite the top 5 vectors remains the same, UDP flooding has dropped from 1st in attack frequency to 5th in terms of attack scale.



ATTACK SCALE | BY SIZE

According to the observed DDoS attack events from 2020, the peak rates of a single attack were recorded between 1Gbps and 10Gbps, with the average value falling at 5.5Gbps.

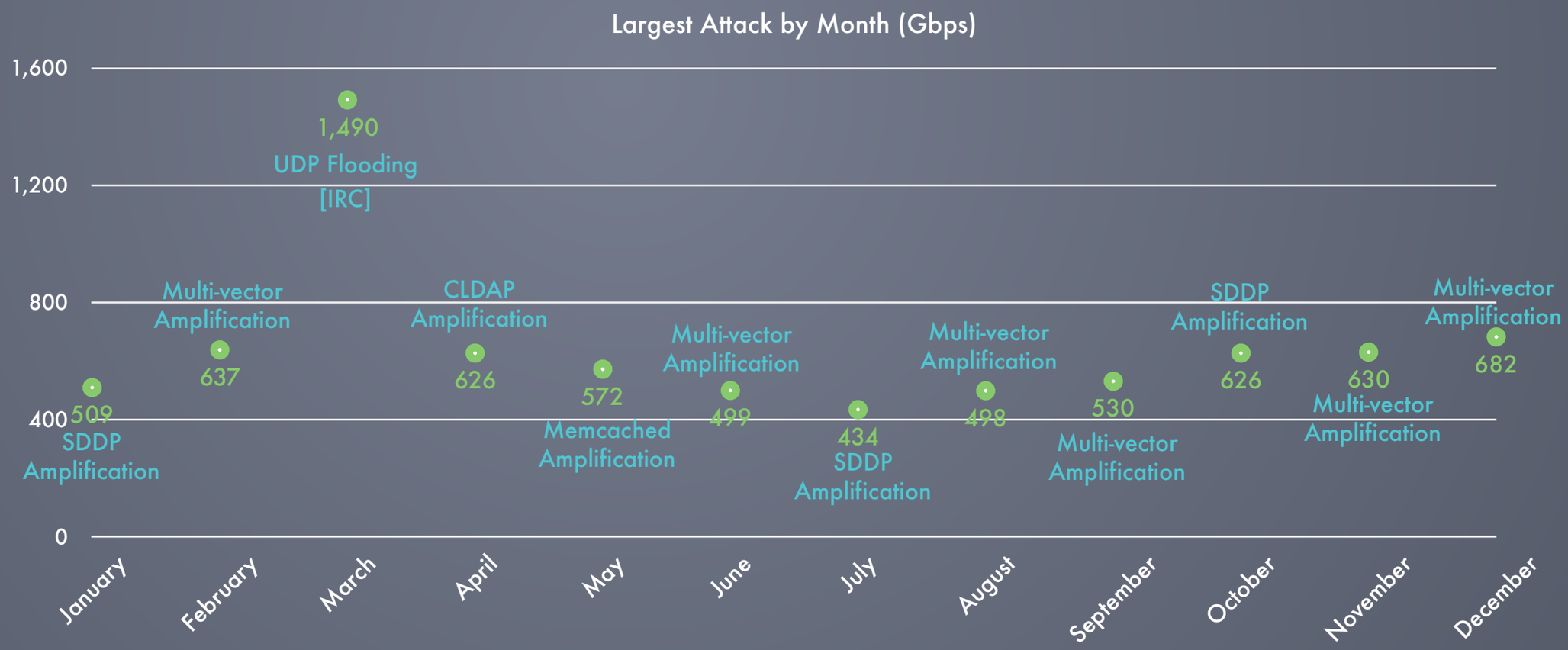
We further analyzed the scale of a single attack among different attack vectors and found that the average peak size of a single attack could vary extremely among different attack vectors. The attack vectors with a large average peak size include reflection amplification attacks, TCP SYN flood, and Malformed TCP or UDP packet attacks, all of which with an average size of 20Gbps or higher. Attacks with a smaller average peak size include worms and specific protocol misuse attacks, which have an average size of less than 100Mbps. Notice that the difference in attack size between large-scale and small-scale attacks can reach up to several hundred times.



VOLUMETRIC ATTACKS | BY MONTHLY TREND

We recorded the attack vector and the size of the largest attack for every month. The below chart shows that for every month of 2020, with the exception of March which was the largest attack incident with 1.49T bps, the monthly largest attack scale usually falls within the range of 400Gbps and 700Gbps.

In addition, the types of volumetric attacks observed were mostly reflection amplification attacks, or multi-vector attacks comprising multiple reflection amplification attack vectors. The only exception is the UDP flooding against a specific port number which was detected in March. In the following chapters, we will take a further look at a few of the top volumetric attacks in 2020.

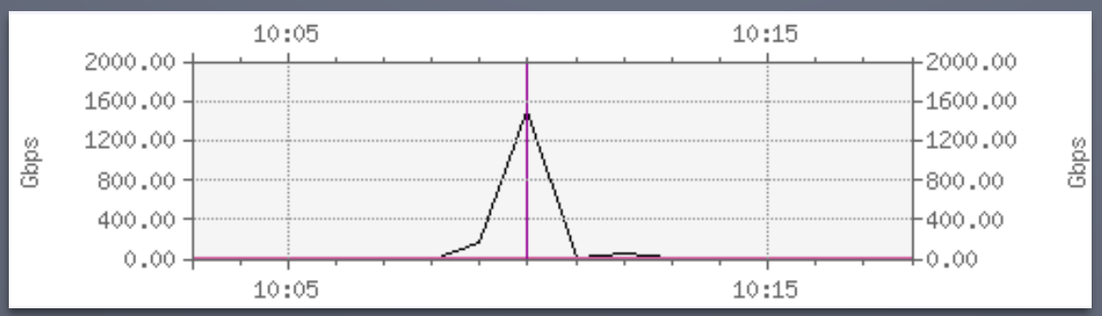


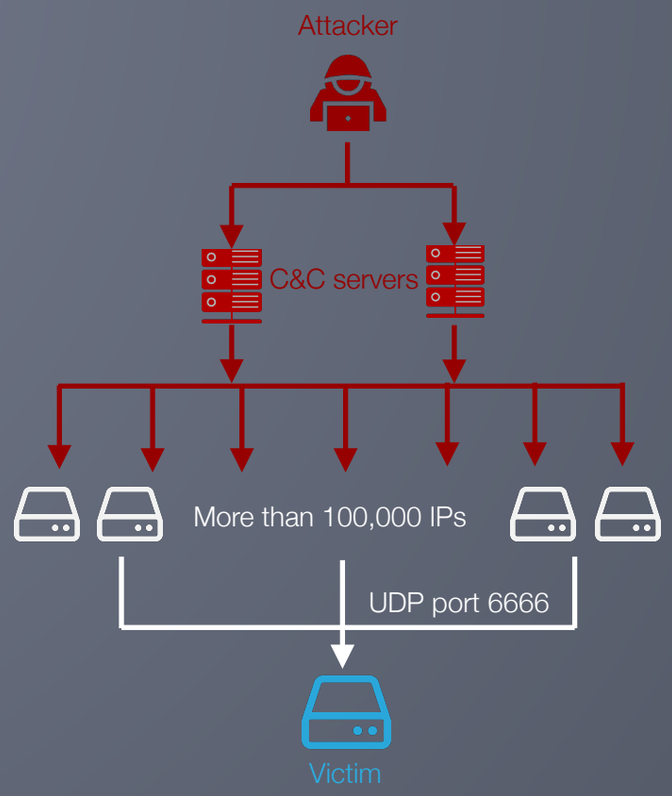
VOLUMETRIC ATTACKS | CASE STUDY 1

The largest attack observed in 2020 occurred at 10:08 on March 22nd, with a peak attack traffic of 1,490G bps and a duration of merely 5 minutes and 26 seconds. The attack is a large-scale UDP flooding with extremely scattered source addresses. The victim's network was flooded by over ten routers, with the attack traffic reaching a peak rate of nearly 1.5T bps within just two minutes. During the peak of the attack, it was estimated that over 100,000 attacking IP addresses were simultaneously sending packets around 408 Bytes to UDP port 6666 of the victim host. The victim host was a server in a cloud service center, and the source addresses of the attack traffic all came from the APAC region.

Let's take a closer look at the traffic behavior of this attack: the UDP port 6666 used in this attack is generally used for Internet Relay Chat (IRC) communication, which is usually used to transmit data in the form of text under the client-server model. The UDP port 6666 is often one of the protocol ports used by the Kali Linux trojans. During the event, the single victim host was attacked by more than 100,000 source IPs sending traffic packets at a speed higher than 3.6Gpps. This is considered a very large-scale Botnet attack.

A botnet is defined as many Internet-connected devices penetrated by malware. Hackers often use botnets as remotely controlled devices to launch a volumetric attack. The power of a botnet is primarily determined by the number of penetrated devices. In the past, to successfully launch a DDoS attack had not been easy. But with the advancement of the Internet of Things (IoT), the number of Internet-connected devices has increased dramatically, and their relatively lower security standards have given botnet hackers a great opportunity to invade. Take the volumetric attack in March for example, tens of thousands of source IPs being launched simultaneously to produce Tb-level attack traffic is undoubtedly a perfect scenario of an IoT botnet attack.



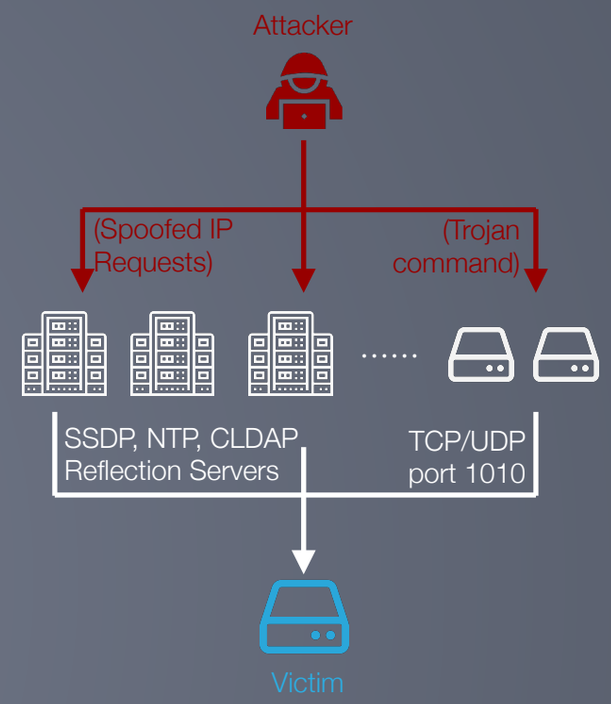


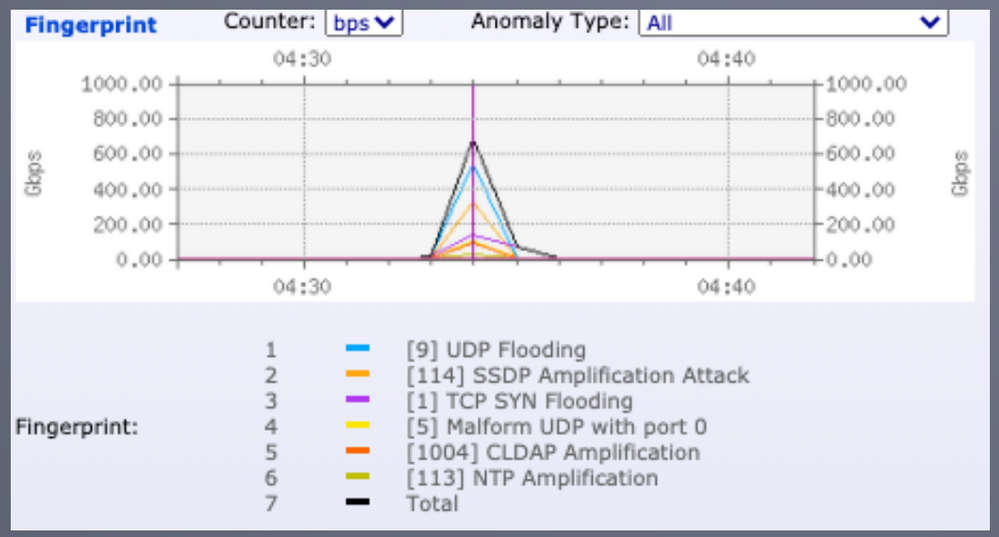
VOLUMETRIC ATTACKS | CASE STUDY 2

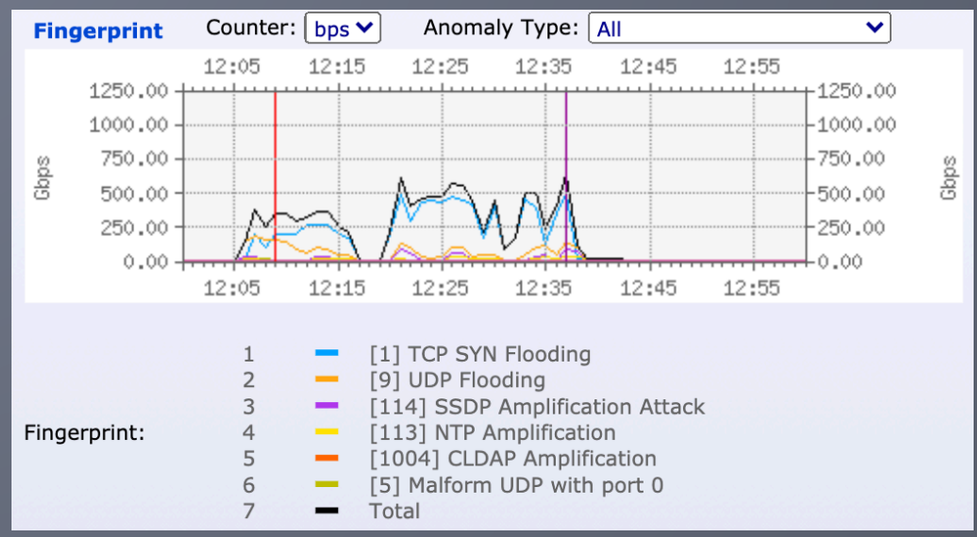
The second and third largest attacks of 2020 were both large-scale multi-vector attacks, which happened at 04:00 on December 3rd and 10:00 on February 12th with a peak traffic of 682Gbps and 637 Gbps respectively. In attack duration, the second largest attack lasted for only about 5 minutes, while the third lasted for 42 minutes.

These two large-scale multi-vector attacks combine several common reflection amplification attacks - including SSDP reflection amplification, NTP reflection amplification, CLDAP reflection amplification, and Malformed UDP packet as a result of a reflection amplification. Other than reflection amplification, these attacks also include a considerable amount of TCP SYN flood attack traffic targeting at port 80, and a Doly trojan based on the source port traffic of several high port numbers targeting a specific TCP/UDP 1010 destination port.

During the peak of these attacks, it is estimated that hundreds of attacking IP addresses used different communication protocols (TCP, SSDP, NTP, CLDAP, etc.) to inject attack traffic into the victim networks through dozens of route links. The source addresses of these two attacks were from domestic carrier networks and both domestic and abroad networks of the APAC, respectively.



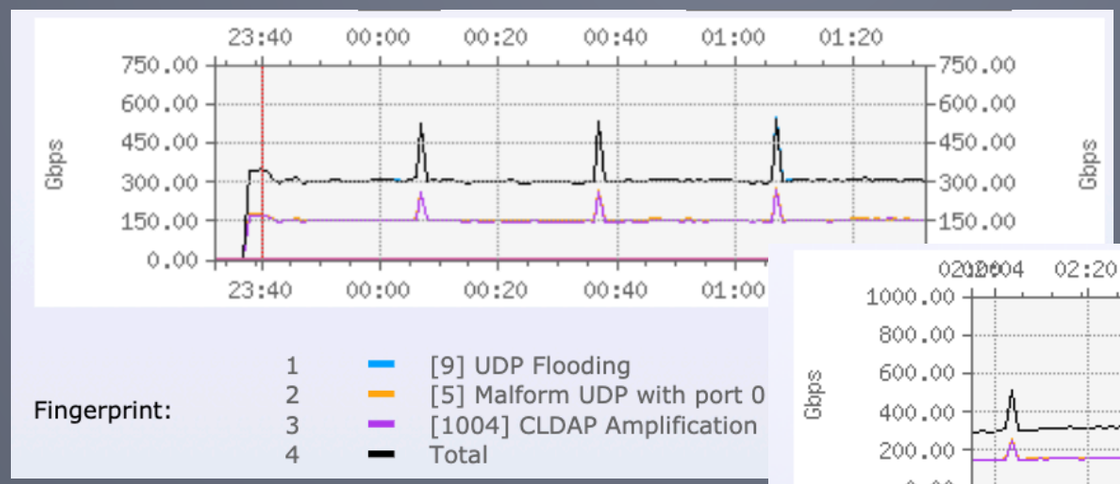


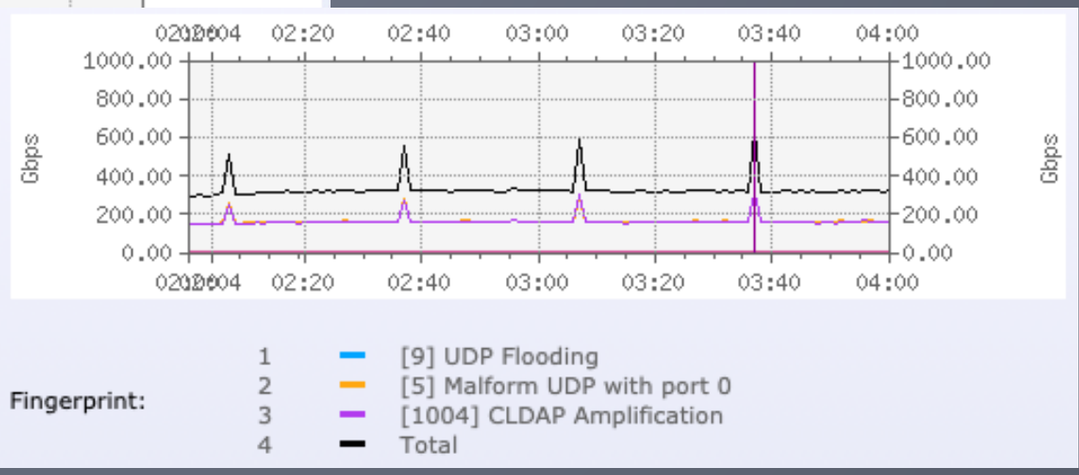


VOLUMETRIC ATTACKS | CASE STUDY 3

The fourth largest attack observed in 2020 was launched at 23:37 on April 18th with a peak rate of 626Gbps. This attack is a large-scale CLDAP reflection amplification attack, accompanied by a large amount of Malformed UDP packet traffic. The attack traffic reached a short-term peak half an hour after being detected. During its peak, it was estimated that more than a thousand reflection servers used the CLDAP protocol to attack the victim host.

Compared with the top three volumetric attacks, this attack had three other special characteristics: First, its attack source mainly came from reflection servers of foreign operators - such as Microsoft, Amazon, Sweden, South Africa, etc.; secondly, the attack lasted for 3 days and 11 hours then returned to a normal level; finally, this reflection amplification attack traffic was not constantly at high flow rate, but rather a pulse wave attack with traffic spikes occurring in clockwork-like succession. In this event, we observed traffic spikes occurring every half an hour, with the peak rates reaching more than 600 Gbps. The burst lasted for about three days, gradually died down and remained at a high flow rate for another three days, then finally returned to normal.





CONCLUSION

In 2020, the number of recorded volumetric DDoS events reached 3.7 million, with an average of 300,000 events per month. The largest attack recorded had a size of 1.5Tbps, and the longest attack lasted for 3 days. In attack frequency, UDP Flooding is ranked at the top with over 30% among all attack vectors, while reflection amplification was the most observed among attack category. TCP SYN flooding was recorded most among attack scale. In average, most peak attack sizes fell between 1~10Gbps, while those larger than 100Gbps also accounted for over 100,000 times. In attack duration, most attacks lasted within 5 minutes, while more than half of the events lasted between 5 to 30 minutes. Attacks longer than one hour accounted for only 10.5%.

Looking at the volumetric DDoS attacks by monthly scale, we found out that the most popular had been multi-vector attacks, which was usually a combination of several reflection amplification attack vectors or even TCP/UDP flood. We also examined some of the top largest volumetric attack cases for 2020, including: Botnet attack driven by IoT devices; Multi-vector attack made up of reflection amplification and flooding attacks; and Pulse Wave attack with traffic spikes occurring in clockwork-like succession.

By examining the statistics of this report, it is apparent that DDoS attacks are becoming more complex and ferocious. Legacy anti-DDoS solutions often fall short to keep up with the challenges brought by these threats. A more effective DDoS security solution must be capable of keeping its pace with evolving technologies to instantly respond, aggregate abnormal traffic, and provide complete detection mechanism at all times.

While the COVID-19 pandemic will eventually come to an end, the advancement of internet technologies has already become a global mega trend. We believe that DDoS attacks will continue to post major threats to telecom and internet service providers. This report should provide telecom network operators a comprehensive understanding of volumetric cyber-attacks and a reference for making network security policies and solution deployment. We hope that the nature of this report can be used as an important resource for the research and development of future DDoS defense solutions driven by advanced technologies like machine learning and AI intelligence. As a trusted partner in carrier-grade network solutions, Genie Networks is standing at the frontline of DDoS attacks for telecom and ISPs with market-leading product lines and insightful analyses.

To provide any feedback on this report, please contact：sales@genie-network.com