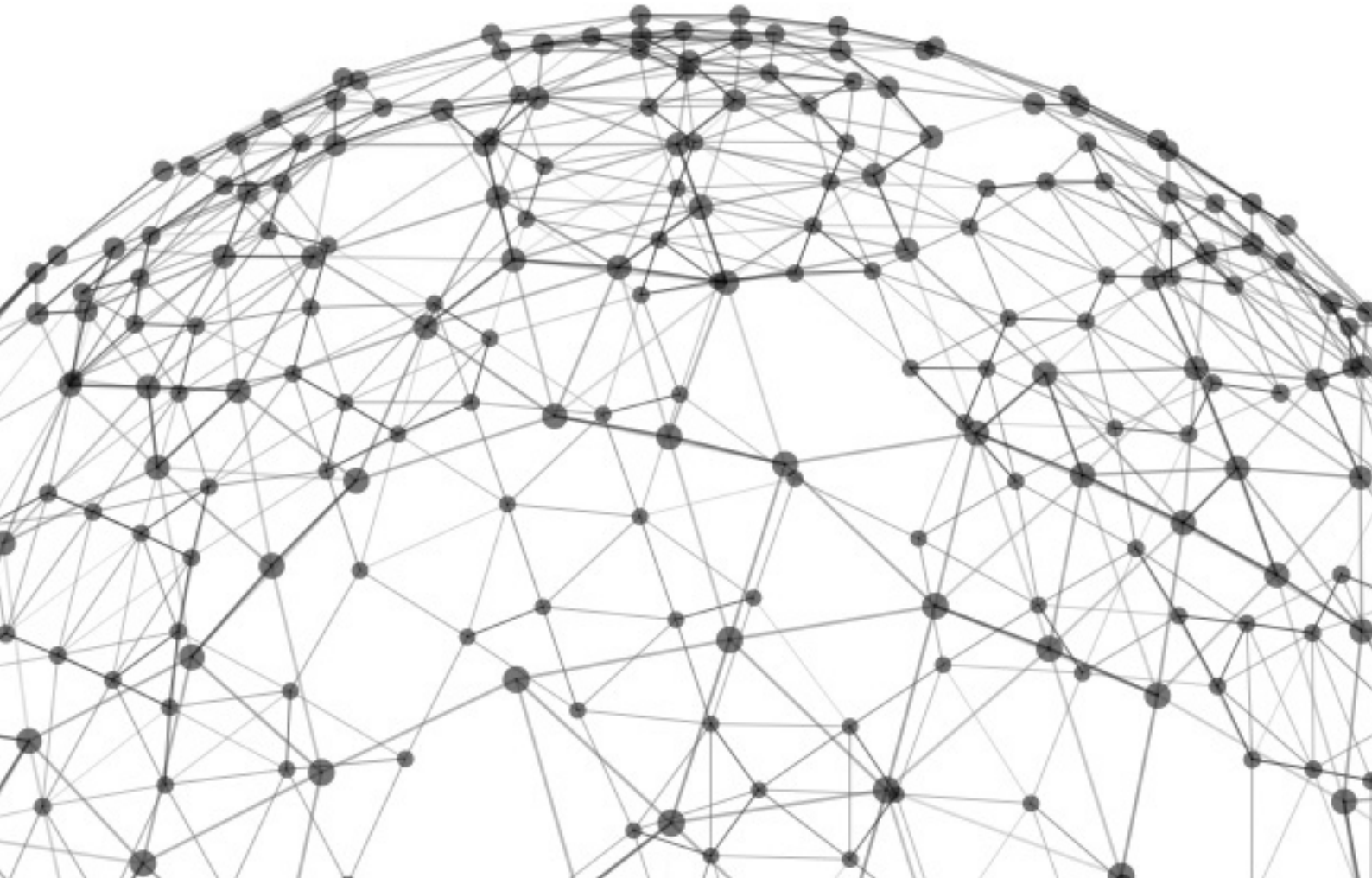
Genie Networks

2021

DDoS Threat Analysis Report

Genie DDoS Security Response Team



Contents

Preface

Looking back at 2021, DDoS threats showed absolutely no signs of abating as adversaries continued to launch a broad array of attacks against organizations. As remote working and online activities officially became the 'new normal' following the pandemic, the trend of digital transformation and advancement of new technologies such as 5G, IoT, and blockchain have fueled a widespread DDoS crisis in which threat actors found a myriad of new attack opportunities.

DDoS activities continued to surge throughout 2021, with total attack traffic hitting record high. Attack scale and magnitude both saw dramatic increase, while attack methods have become vastly more sophisticated. The number of Tbps-scale attacks rose significantly as compared with 2020. More multi-vector attacks were observed, among which a record-breaking largest attack in a single month has been reported.

Standing at the forefront of network traffic analysis and DDoS protection, Genie Networks possesses the key statistics and data of the latest DDoS threats studied and collected by our Genie DDoS Security Response Team. This report uncovers the data of 2021 from several Tier-1 service provider networks in the APAC region, including those of telecom carriers, internet service providers, data center/co-location providers, and mobile network operators. Since Genie's product specializes in L3 and L4 volumetric attack detection, this report is primarily focused 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 couple of the largest volumetric attack cases in 2021.

As cyberattack continues to grow and disrupt at the same rate as modern technology, we can only expect record-breaking numbers in the years to come. In the post-pandemic world, safeguarding against DDoS threats is imperative for any organization to maintain competitive and sustainable in a highly-evolving digital landscape. We expect this report to not only provide the necessary insights into the latest DDoS trends, but also a reference for organizations on security policy implementation and security measure deployment.

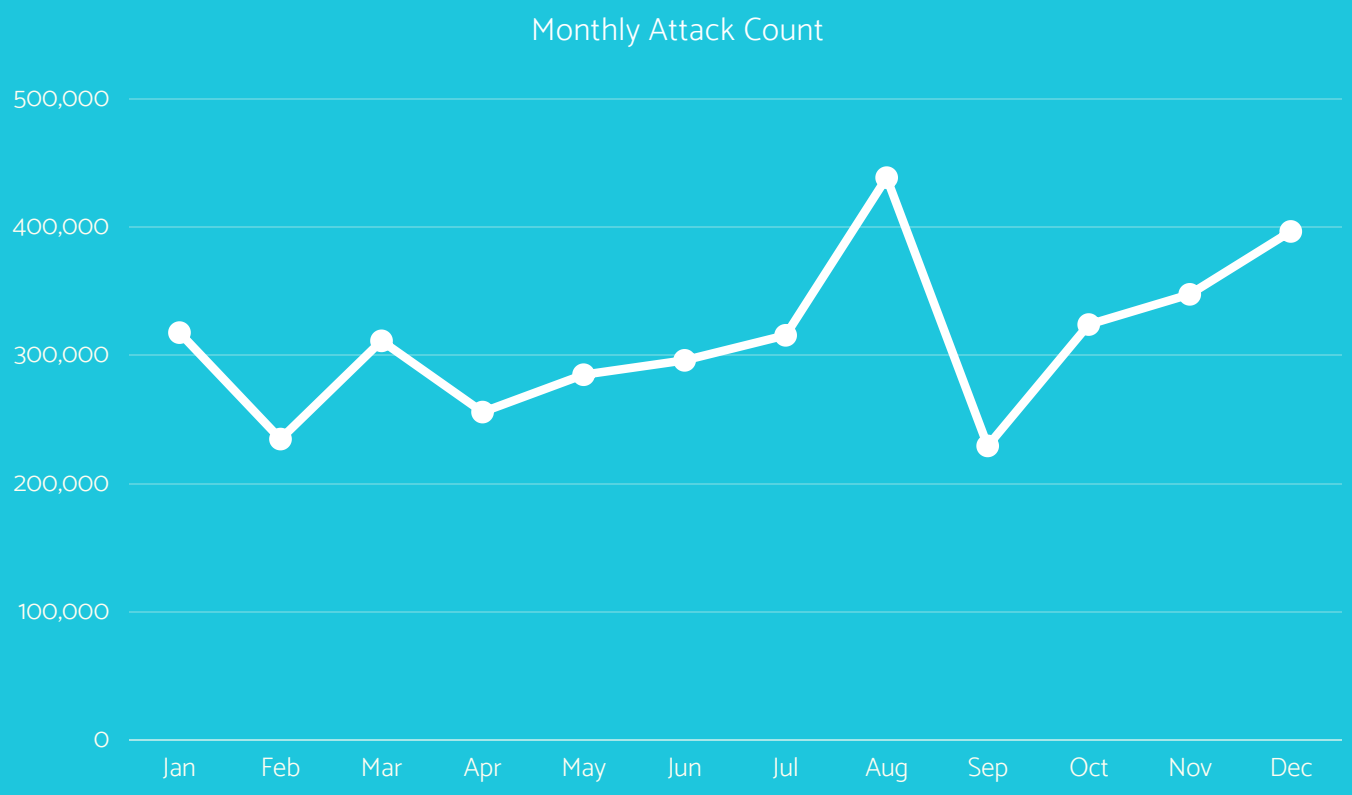
Genie DDoS Security Response Team
2022/3

Attack Frequency

Overall Trend

In 2021, Genie DDoS Security Response Team observed a total number of 3.75 million DDoS attacks. This result is very close to that of 2020, which observed a number of 3.70 million attacks. The attack count observed each month falls between 220,000 to 640,000, with the highest at 440,000 in August, and lowest at 230,000 in September. The monthly attack frequency fluctuates at a considerable degree, with a growth/decline range (MoM+) between -50% and +50%. On average, 310,000 attacks were observed each month, indicating:

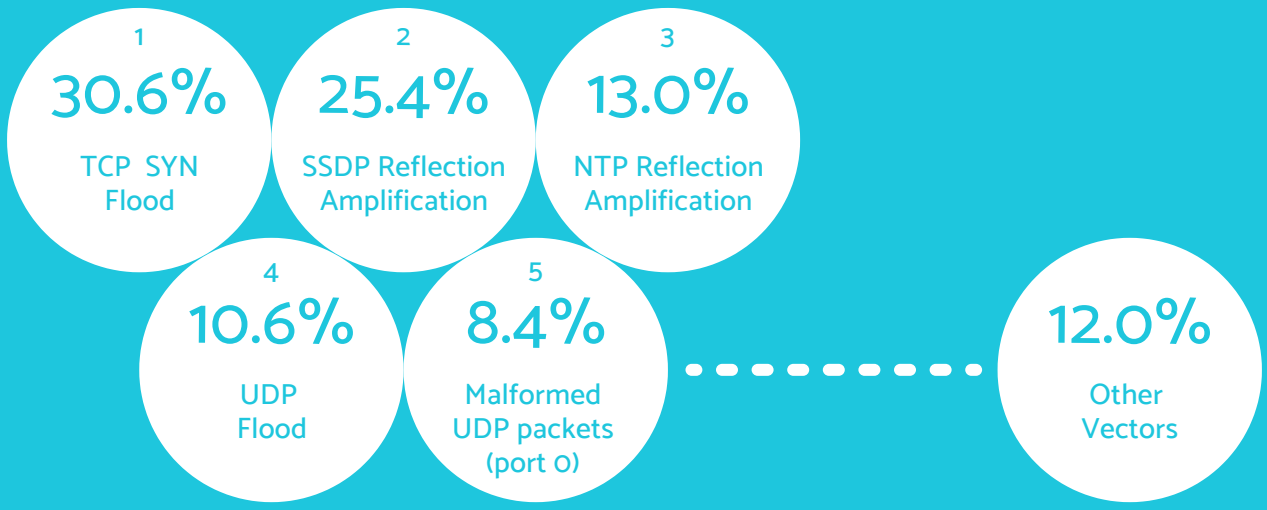
- 10,283 attacks per day,
- 428 attacks per hour,
- and 7 attacks per minute.



Attack Frequency By Vector

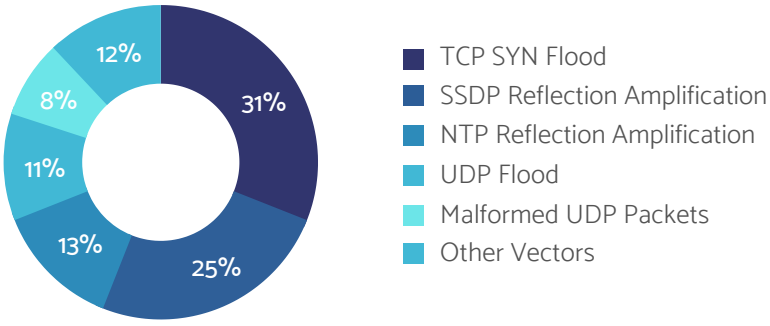
We observed different types of DDoS attack vectors that can be divided into the following categories: TCP flood attacks (such as SYN Flood, RST Flood, SYN-RST Flood... etc.), UDP flood attacks, protocol misuse attacks (such as Malformed TCP packets, Malformed UDP packets, Land Attack, IP Protocol Null, 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.

By attack count, the top 5 DDoS vectors for 2021 are:



In total, the most common attack vector for 2021 is reflection amplification, then followed by UDP Flood and TCP SYN flood.

Highest Frequency by Attack Vector

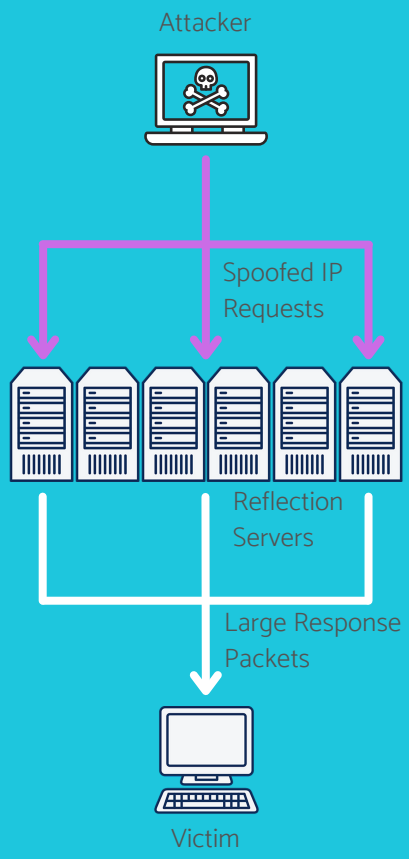


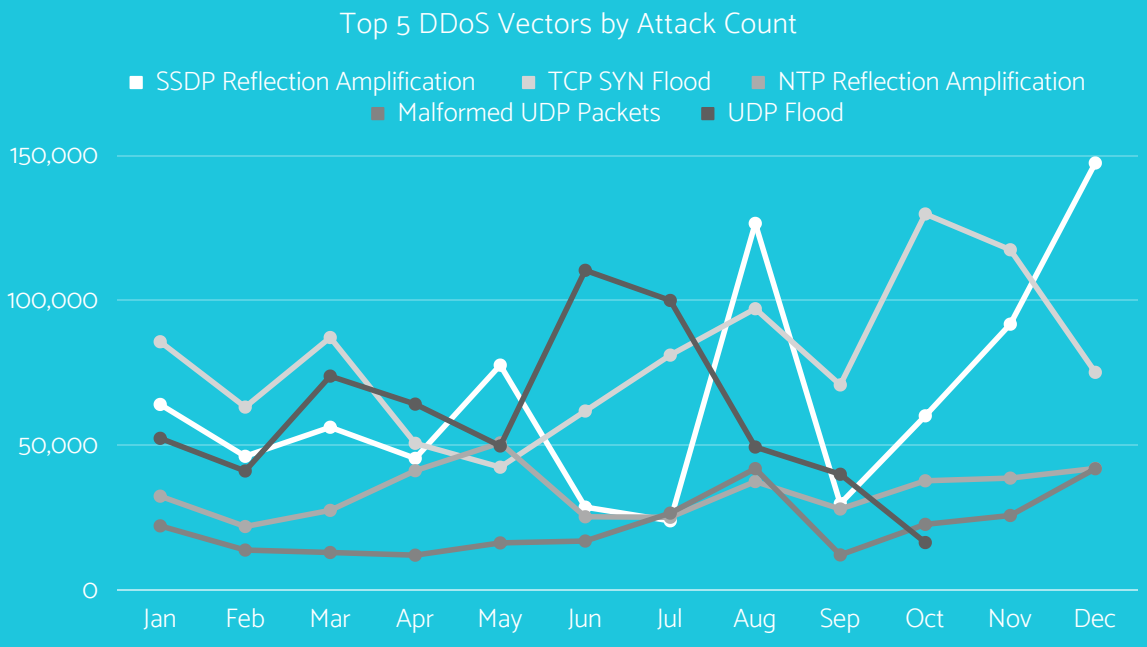
The top 5 most observed attack vectors in 2021 were nearly the same as 2020 except for a slight change in ranking and percentage. TCP SYN flood tops the list (from 18.2% in 2020 to 30.6% in 2021) while SSDP and NTP reflection amplification both surpassed UDP Flood compared with the previous year.

Attack Frequency by Vector Trend

The Top 5 Monthly Attack Vectors in 2021 saw little change relative to the previous year. Other than DNS reflection amplification attack reaching top-5 in November and December, 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 an attack like SSDP or NTP reflection amplification, the reflection servers usually respond to the attacker's Spoofed IP requests with extremely large UDP packets of 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 whose source/destination port number equals 0. In summary, an often scenario with high-ranked Malformed UDP packet usually indicates a high chance of a reflection amplification attack.

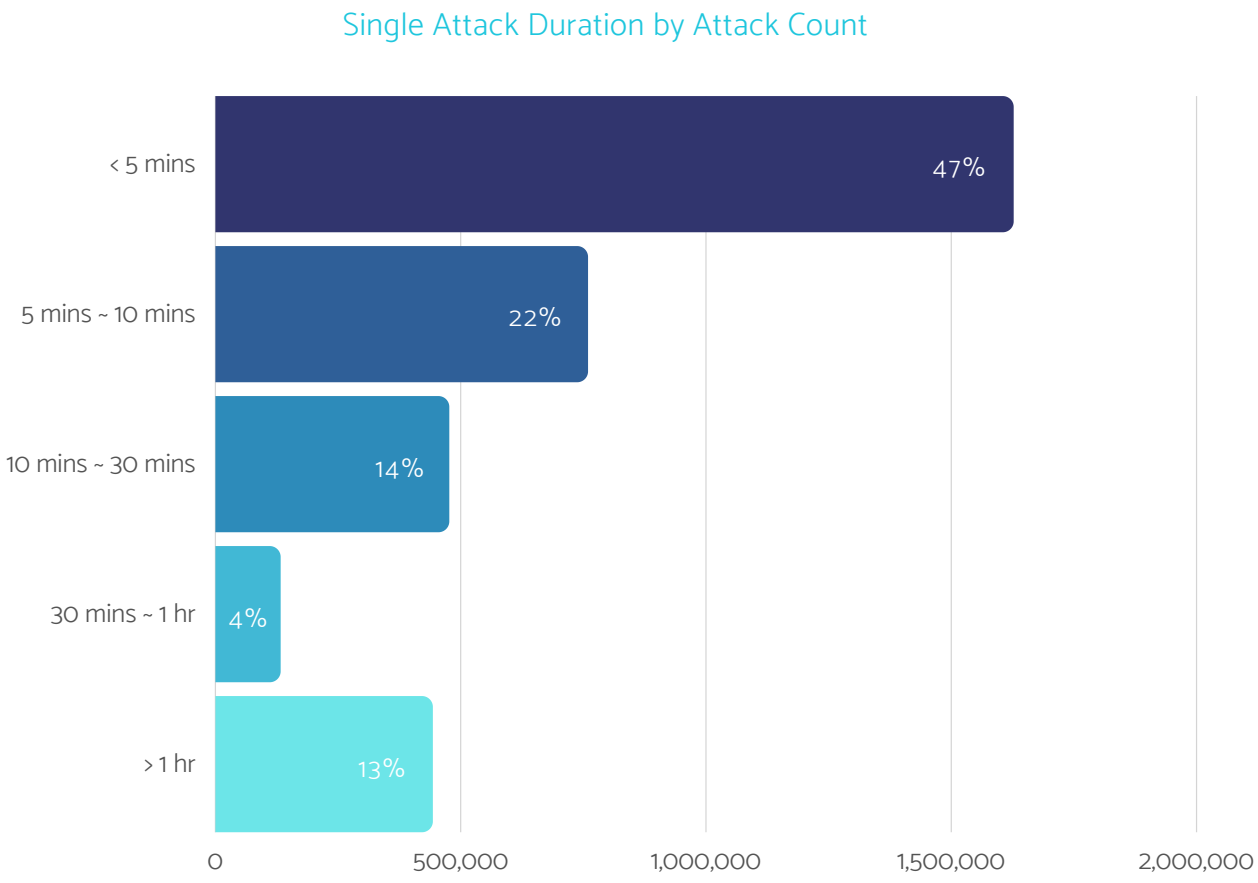




Attack Frequency By Duration

The average attack duration recorded for 2021 is 62.7 minutes.

About half of the recorded attack events lasted within 5 minutes, and around 36% lasted between 5 to 30 minutes. While attacks that lasted more than an hour accounted for only 13%, the overall average attack duration still lasted an hour long. This is because the number of attacks longer than one hour usually took much more than an hour, and 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 early initialization stage.



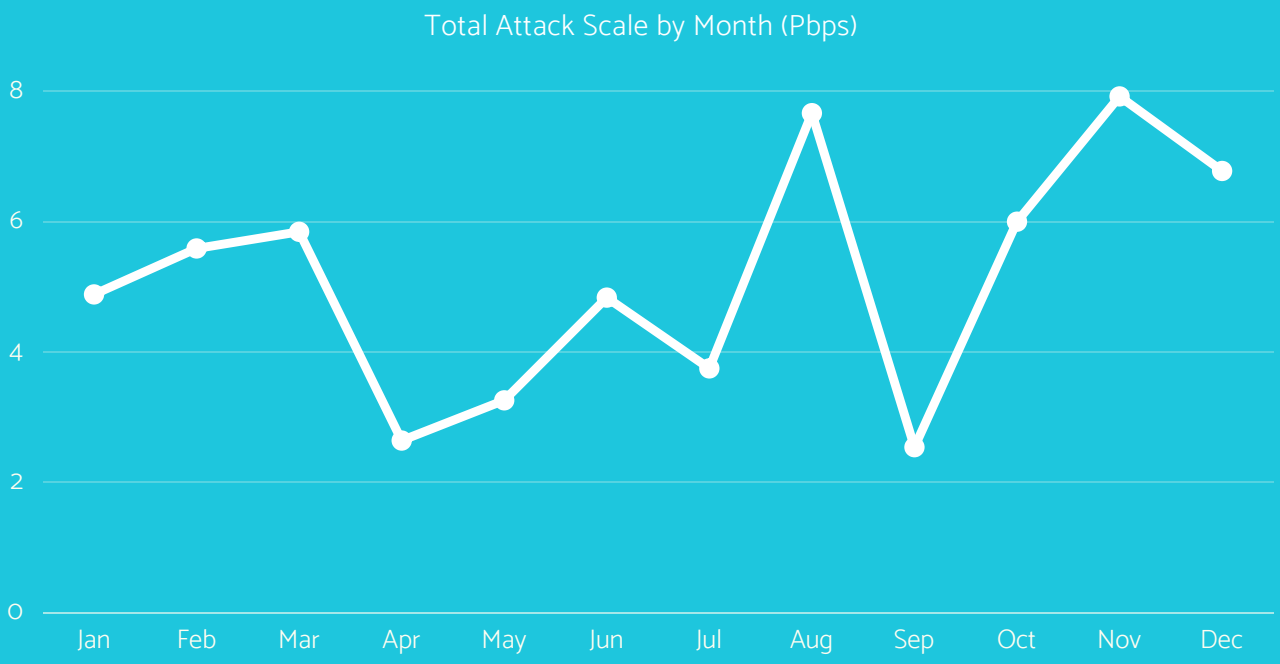
Attack Scale

Overall Trend

In 2021, our DDoS Security Response Team observed a total attack traffic of 61.7 Peta bps. The observed monthly attack scale falls between 2 Pbps to 8 Pbps, with the highest at 8 Pbps in November and lowest at 2.5 Pbps in September. The monthly attack scale fluctuates at a considerable degree, with a growth/decline range (MoM+) between -70% and +140%. On average, 5.1 Pbps of attack traffic were observed each month, which indicates:

- 169 Tbps of attack traffic per day,
- 7 Tbps of attack traffic per hour,
- and 117.4 Gbps of attack traffic per minute.

In 2021, the observed total attack traffic grew 21% compared with last year, which is significantly larger than the growth in attack count (1.3%) from 2020 to 2021. This can be explained that the scale of each single attack observed in 2021 had been significantly larger than the previous year.



Attack Scale By Vector

The top five attack vectors of 2021 based on attack scale are:

1
30.1%
TCP SYN Flood

2
25.6%
SSDP Reflection Amplification

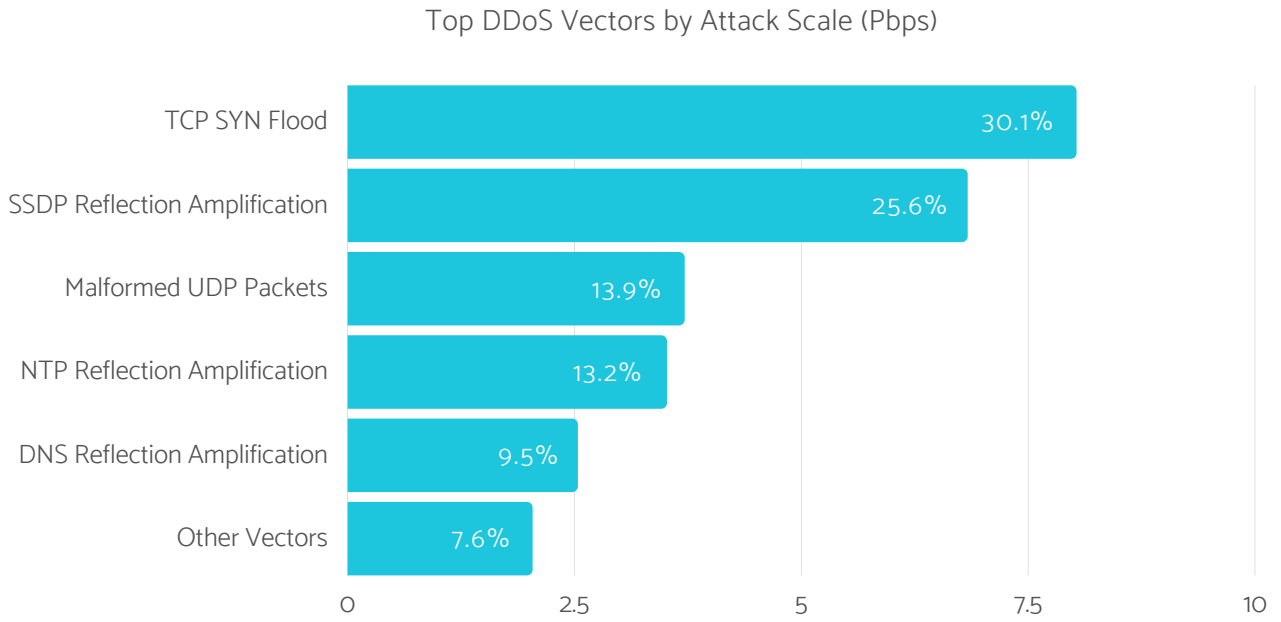
3
13.9%
Malformed UDP Packets (Port 0)

4
13.2%
NTP Reflection Amplification

5
9.5%
DNS Reflection Amplification

7.6%
Other Vectors

Notice that the top 5 attack vectors by scale in 2021 closely resemble the top 5 vectors by attack count (notably the first and second being TCP SYN Flood and SSDP Reflection Amplification with almost identical percentages).

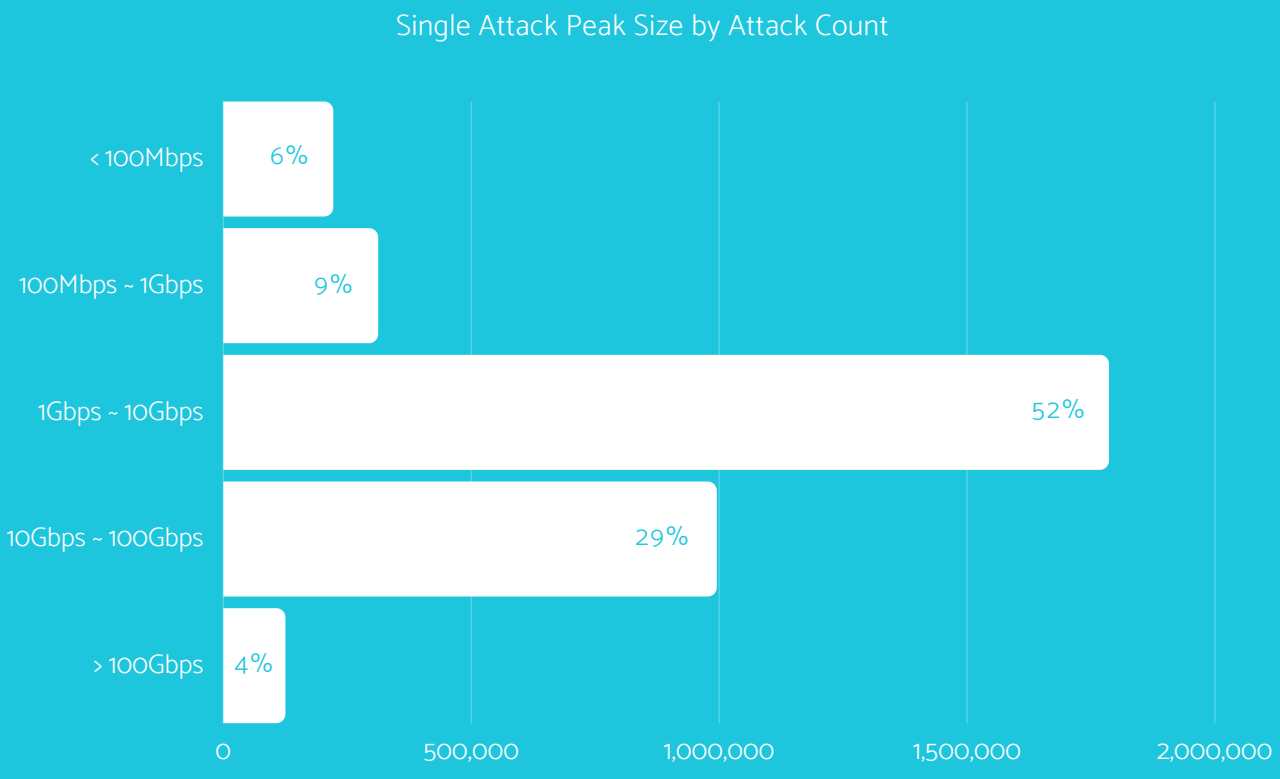


Attack Peak Size

According to the observed DDoS attack events from 2021,

- An average single attack peaks at 17.5 Gbps
- Most attacks peak between 1 Gbps to 10 Gbps

Further analyzing the scale of a single attack among different attack vectors, we found that the average peak size of a single attack could vary extremely among different attack vectors. Attack vectors with a large average peak size include IP Protocol misuse (null) attack, Memcached attack, reflection amplification attack, Malformed TCP or UDP packet attack - all with an average size of 50Gbps or higher. Attack vectors with a smaller average peak size include worm attack and specific protocol misuse attack, which have an average size of around hundreds of Mbps.



Attack Source by Geography

Among all observed DDoS events in 2021, most attack source IPs came from China (24.6%), followed by USA, Hong Kong, Japan, Singapore, Australia, etc.

Note that the observation of attack source location is based on data collected on the source IPs of the attack traffic, which may not genuinely reflect the actual location of the attacker. For example, adversaries may use Source IP Spoofing to generate fake requests in order to evade security systems. Steps to detect IP spoofing include deploying packet filtering and network topology configuration. This report, however, has not taken such measures considering its scope which covers across a broad range of service provider networks.

For the purpose of this report, during a reflection amplification attack, the attack source IP location refers to the location of the reflection servers (as shown in Figure 1); and in a botnet attack, the attack source indicates where the compromised bots are (as in Figure 2), instead of the actual location of the attacker's C&C servers.

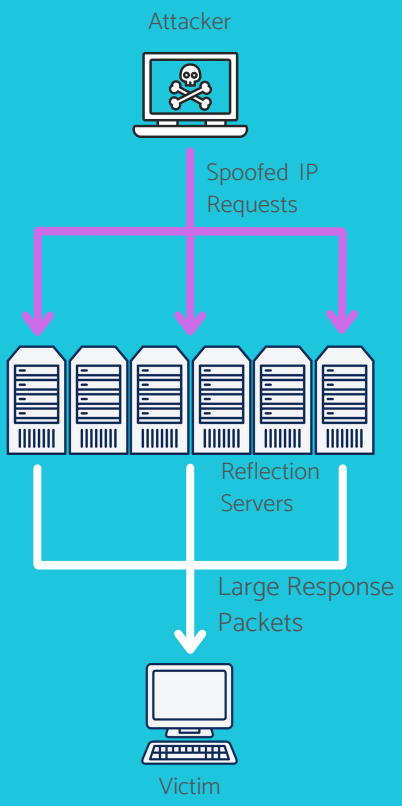


Figure 1

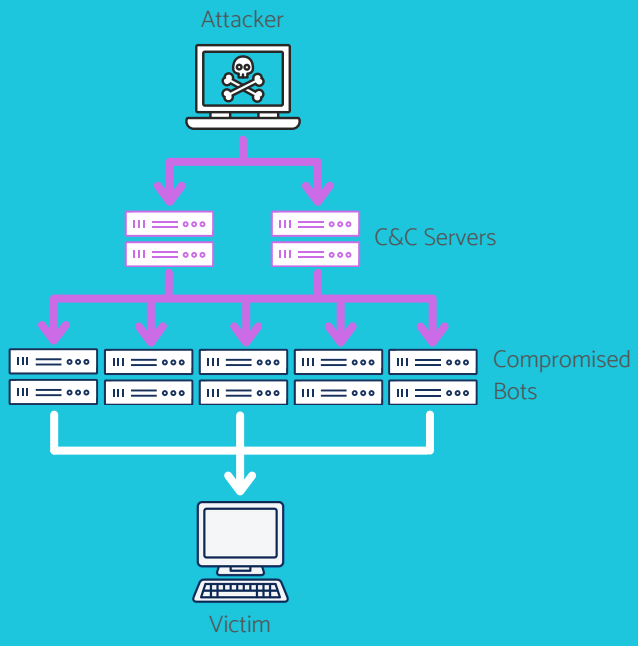
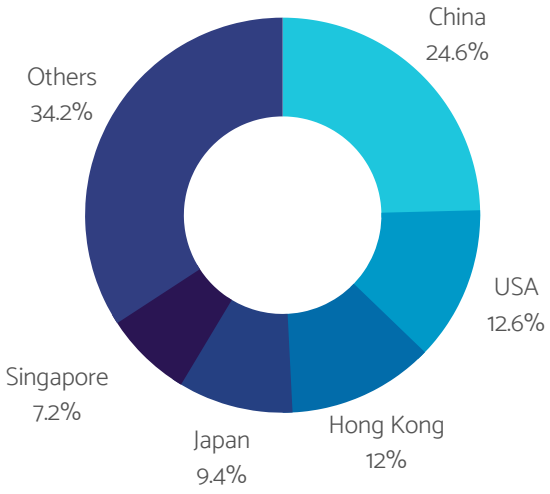


Figure 2

Attack Source by Region



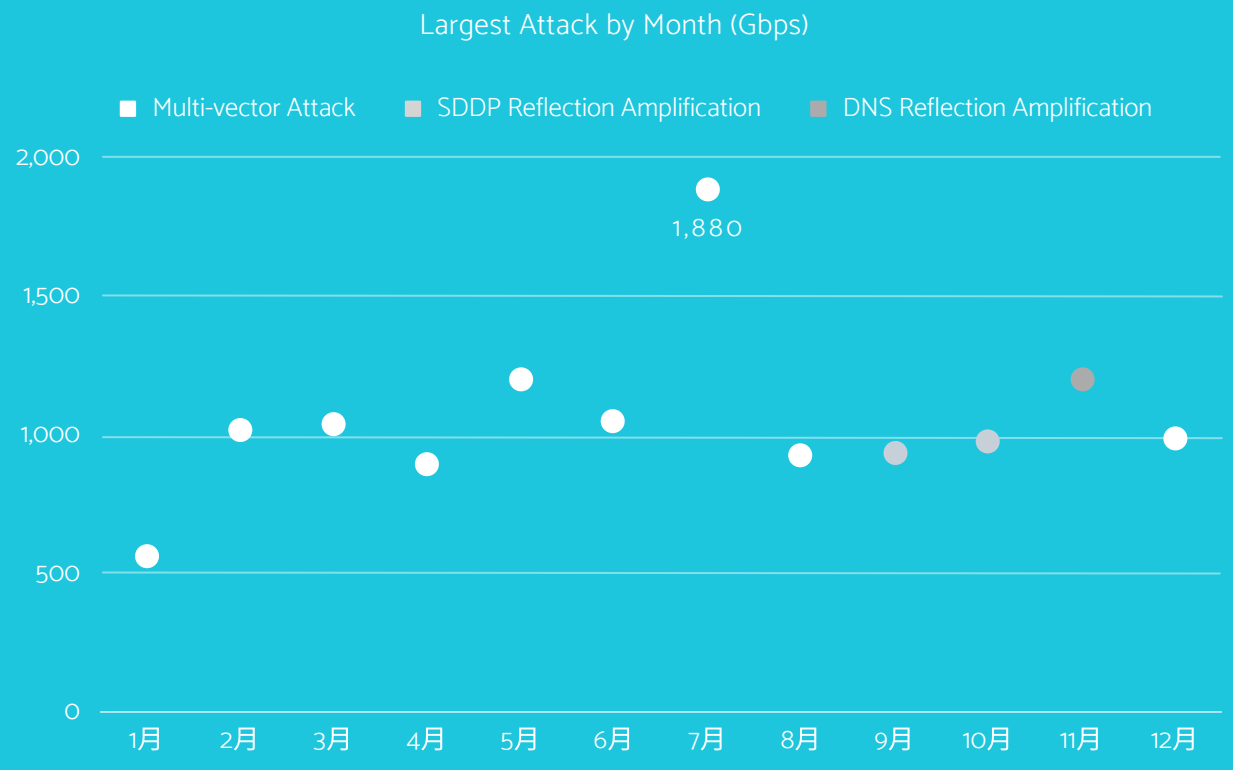
Volumetric Attacks

Monthly Trend

Observing the size and vector of the largest attack for each month, we found the largest attack in 2021 occurring in July, with an attack scale of 1.88 Tbps. In average, the largest attack each month generally falls between 500 Gbps to 1.2 Tbps.

The scale of volumetric attacks in 2021 increased significantly by 65% against the previous year.

In 2021, the types of volumetric attacks observed were mostly multi-vector attacks comprising UDP reflection amplification attacks, or other types of reflection amplification attacks such as SDDP and DNS reflection amplification. We also found that among all the multi-vector attacks observed in 2021, TCP Flood has also been used often to create volumetric attacks, aside from the often-seen UDP reflection amplification.



Volumetric Attacks

Case Study 1

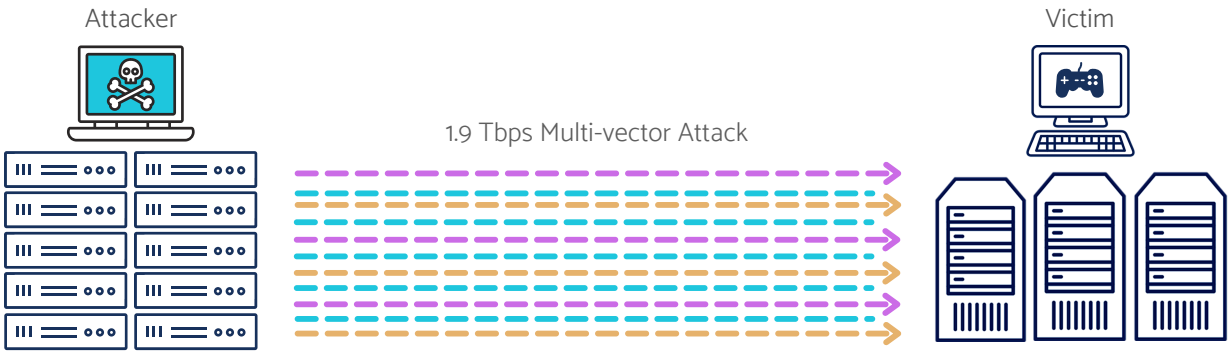
The largest attack observed in 2020 occurred at 07:59 on July 12, with the following characteristics:

- Peak attack traffic up to **1,880 Gbps**
- Duration of 8 minutes and 3 seconds
- A multi-vector attack

The attack primarily consists of SSDP reflection amplification, combining with DNS reflection amplification, NTP reflection amplification, CLDAP reflection amplification, UDP flood, and TCP flood attacks. The victim's network was flooded by routers across over 10 points of entry, reaching a peak rate of nearly 1.9 Tbps within just two minutes. During the peak of the attack, it was estimated that hundreds of attacking IP addresses were simultaneously sending packets up to Giga Bps to UDP/TCP port 80 of the victim host.

Taking a further look into this event, we found that the same victim host was not only attacked particularly on July 12, but was constantly being targeted by Tbps-level volumetric attacks more than ten times within two weeks of that timespan. These attacks could be the same multi-vector combination as mentioned earlier, or simply a UDP Flood which also sends packets up to Giga bps to UDP/TCP port 80 of the victim host. The duration of these attacks all ended within ten minutes.

The victim host is one of the cloud servers of an online gaming service provider which is often targeted by DDoS threat actors. Although attacks have been observed throughout the year, we found that most events, typically those with the greatest attack size, occured in June and July.



Volumetric Attacks

Case Study 2

UDP is often known as the most common type of protocol to execute volumetric DDoS attacks. This is because, in contrast to a stateful protocol like TCP, UDP can be easily exploited by adversaries to elicit amplification reflection servers with only a slight amount of traffic to send amplified attack traffic to the target IP address. This means UDP traffic runs with less overhead to effectively exhaust the victim's bandwidth. The ratio of the size of the spoofed IP requests initiated by the attacker to the response packets returned by the reflection amplification server is known as the amplification factor. Based on the observed UDP reflection amplification events in 2021, we ranked them in the chart below according to their total volume of attack traffic and showed their amplification factors.

From the chart, we notice that despite a bigger amplification factor should contribute to a more effective attack vector, the ranking of the attack vector does not necessarily correspond to that of the amplification factor. This implies that factors other than the amplification factor need to be taken into consideration as well, such as if the reflection amplification servers can be easily exploited and weaponized.

TCP, on the other hand, is less vulnerable to abuse than UDP since it requires a three-way handshake. Although the amplification factor and generated attack traffic of its reflection amplification attack is less effective than that of UDP, we have been witnessing cases of TCP reflection amplification attacks every once in a while. A TCP reflection amplification attack is leveraged to create high packet rates (packets per second - PPS) that elicits large amplification factors capable of overwhelming the targeted server. An example is a new form of TCP reflection amplification attack that was disclosed at the 2021 USENIX Security Conference - known as the TCP Middlebox Reflection Attack. It involves abusing the vulnerabilities of firewalls and DPI systems to reflect and amplify TCP traffic to the victim, generating a ferocious DDoS attack. Though the amplification factor of such an attack varies upon the status or brand of the middlebox, it is generally understood to create amplification factors around 100x~200x, and even at highest up to 50,000x. This is definitely an attack vector to pay attention to for 2022.

Attack Traffic Rank	Attack Vector	Amplification Vector
1	SSDP	~28X
2	NTP	~200X
3	DNS	~100X
4	CLDAP	~50,000X
5	Memcached	~60X
6	SNMP	~600X
7	Chargen	~400X

Conclusion

In 2021, we observed just minimal growth (YoY+ 1.3%) in the number of volumetric DDoS attacks. Instead, we witnessed a 21% YoY growth in total attack traffic and apparent growth in the scale of single attacks throughout 2021. This also implies to mega volumetric attacks, with a record up to 12 attack counts in 2021 compared to only 1 in 2020.

Looking at the attack vectors for 2021, flood attacks continue to dominate aside from a few types of reflection amplification attacks (ex. SSDP, NTP, etc.) and their fragmented traffic (UDP port 0). In attack size, most peaks reach 1 to 10 Gbps, while attacks greater than 100 Gbps also accounted for a whopping 123,852 times. In attack duration, more than half of the recorded events ended within 5 minutes. Looking at the trend of the largest attack for each month, multi-vector attacks are undoubtedly predominant. They are often combinations of multiple reflection amplification attacks and TCP/UDP flood attacks.

Through this analysis report, we can clearly see the unstoppable menace of DDoS attacks. The magnitude of these malicious traffic not only cause service downtime or outages for the targeted victim, but could also vastly damage the network resources provided by the victim's service provider. In some cases, the devastation could even spread to the service provider's other customer networks. As a DDoS attack is often launched from multiple compromised devices, it is often challenging for legacy in-line security solutions to effectively guard against these highly-evolving threats. Rather, these systems often fall victim to a DDoS attack themselves due to their vulnerability. Therefore, an Out-Of-Path (OOP) solution with network-wide real-time detection and mitigation features has now become a de facto standard for modern DDoS security.

Since its establishment in 2000, Genie Networks has been at the forefront of carrier-grade network traffic analysis and DDoS protection. Our GenieATM has provided countless Tier-1 Telcos, ISPs, and large enterprises with the best-of-breed OOP solutions to ensure network visibility and safeguard against DDoS threats. Explore our products and solutions at www.genie-networks.com or contact us directly at sales@genie-networks.com.