ATTACK CAMPAIGN

2023 DDoS Attack Trends

We analyzed the last three years of DDoS data, and found attackers shifting to more complex approaches, and shifting up the stack.

By Malcolm Heath (additional contributions by Sander Vinberg)

February 21, 2023 • 15 min. read

Table of Contents

As we have done for prior DDoS Attack Trends reports, we recently analyzed attack data from the F5 Distributed Cloud DDoS Mitigation service to get a look at the DDoS traffic they handled for their customers in 2022. We continued our analysis by comparing 2022 data to that of 2021 and 2020. Some interesting trends emerged.

Executive Summary

- Application layer attacks up by 165%
- The Technology sector takes the top spot as most attacked over 2022
- Overall observed events are down by -9.7%
- Peak Bandwidth up 216% from 2020
- All verticals should expect to see more Application and Multi-vector DDoS

Terms To Know

Volumetric Attack

Volumetric attacks use a variety of techniques to attempt to overwhelm the available bandwidth at the target. Such techniques include UDP floods, ICMP floods, and reflection attacks leveraging protocols such as NTP, Memcached, and DNS to amplify the amount of traffic received by the target.

Protocol Attack

Application Attack

Multiple Vector Attack

Vital Components

Attack Type:

A Note on the Analysis

Distributed Denial of Service (DDoS) has been an issue for a very long time, and while our defenses have come a long way since the earliest days, such attacks can still be devastating. Attackers continue to use these techniques to annoy, harass, and extort vulnerable targets, so tracking DDoS trends remains an important function of threat intelligence writ large. There are, however, a few things to keep in mind when reading any analysis of DDoS trends and events. Bringing a critical frame of mind to any data to determine relevance to your specific situation is key to being able to turn observations into action. Any dataset relating to DDoS traffic will only show what the collection point was able to observe, and this will be only a fraction of the total DDoS that occurred across the internet.

While the observations may be a small subset of the total landscape of DDoS, we nevertheless feel the trends observed in this data may be broadly comparable to the entire situation, as the F5 Distributed Cloud DDoS Mitigation service protects a diverse group of customers, ranging from small to large enterprises, and from many different industry verticals.

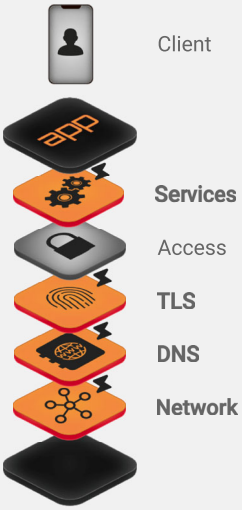
DDoS Attacks

Attack Method:
DNS amplification
SSL-TLS renegotiation
SYN, UDP, and HTTP floods
View all

Attack Motive:
Hacktivism

Malware / Campaign Name:
Killnet
Tofsee Botnet

Affected Tiers



Terms Used in This Report

If you're new to denial of service attacks and would benefit from a detailed look at the types and method of DoS attacks, and the motivations of the many threat actors who use them, take a look at our Learning Center article What is a Distributed Denial-of-Service Attack?

Peak Bandwidth

Nearly all DDoS attacks will have a ramp up and a ramp down period in terms of the bandwidth they use. The peak bandwidth is defined here as the maximum observed bandwidth in a single point in time during the attack. It does not indicate how long the total attack lasted, but does give some indication as to the resources the attacker put towards creating it, and to some extent, its intensity.

Attack Type Classifications

Because there is a large number of specific DDoS attack types, we've broken them out into the following categories. Our classification scheme roughly overlaps with the DDoS terms used by the MITRE ATT&CK framework.

Volumetric

Volumetric attacks use a variety of techniques to attempt to overwhelm the available bandwidth at the target. Such techniques include UDP floods, ICMP floods, and reflection attacks leveraging protocols such as NTP, Memcached, and DNS to amplify the amount of traffic received by the target.

Protocol

Protocol attacks are those that specifically target the ability of network infrastructure to track and handle traffic. Examples include TCP Syn and TCP Ack flooding. These are also known as 'computational' attacks, since they often overload the compute capacity of network devices, such as routers and firewalls.

Application

Application attacks are those that target higher level protocols, the most frequently observed being HTTP GET floods, TLS renegotiation, and DNS queries. We make the distinction here between DNS *reflection*, whose aim is to flood the targets internet connection with query response traffic, and DNS *queries*, which are made directly to the target's DNS infrastructure, with the aim of denying legitimate requests the ability to resolve domain names.

Multiple Vector

We use the term "multiple-vector" for attacks which leverage more than one of the above methods. More details on the specific combinations observed are mentioned in passing in the rest of the report. While many DDoS attacks use a single vector, these multiple-vector methods are becoming increasingly common.

2022 DDoS Insights

In 2022, we saw the overall number of attacks trend down a small amount, and saw a sharp rise in the number of Application layer attacks.

Trend 1: Overall DDoS Attacks Were Slightly Down

In 2022, we note a slight reduction (-9.7%) in the overall events observed from that of 2021, continuing a similar reduction in overall events between 2020 and 2021 (-3.5%). The number of events observed per quarter does not vary much. Q1 2022 was significantly less than the same quarter in the year before, with a 50.7% reduction (Figure 1).

This is perhaps attributable to the beginning of the Russian invasion of Ukraine. At that time, it was noted by several threat research firms that there was significant turmoil among various cybercriminal organizations, as they determined what their approach would be regarding the conflict, and which side, if any, they would align with. Resources were redirected, at least briefly, to support one side or the other of the conflict, and several large-scale DDoS attacks against both Russian and Ukrainian targets made the news. This may account for the drop in Q1 events we observed, but we can't be sure. The overall drop from Q4 2021 to Q1 2022 was -25%.

Politically motivated attacks are ongoing – as this report was being written, widespread DDoS attacks against hospitals were being reported, and attributed to Killnet, a Russian-aligned group which has launched such attacks against several verticals since the war began.[1] Please see the section "Is Killnet a Sign of Things to Come?" below for more details.

The level of attacks ramped back up to approximately normal levels in the following quarters, increasing an average of 30% quarter to quarter, and although the overall yearly totals were down, Q4 2022 showed the highest observed number of events in a single quarter across all three years. See Figure 1.

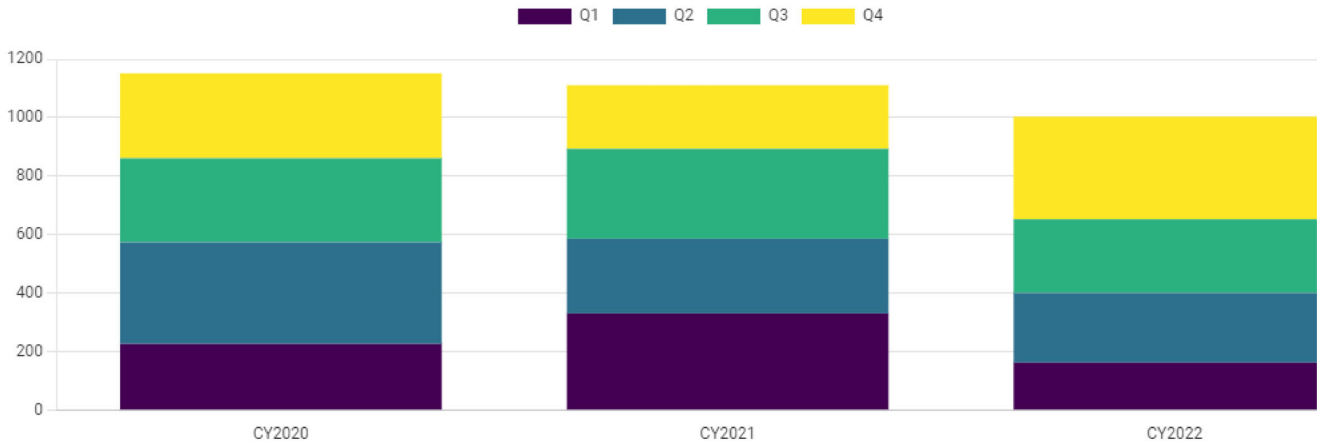


Figure 1 Total DDoS events observed in 2020-2022. Overall number of events went down between 2021 and 2022. Q4 2022 had highest overall number of events

Despite the overall decline in 2022 events, we agree with the consensus opinion that DDoS remains a threat which will grow in the future, with more attacks likely to occur going forward.

In the rest of the analysis, you may note that the numbers of observed events and the totals for various classifications don't seem to match precisely. That is because some events (approximately 70 of them) were unable to be classified according to our scheme of Application, Protocol, Volumetric, and Multi-vector.

Trend 2: Application Vector Attacks are Becoming Far More Frequent

Breaking this out by category, we can see that in 2020 and 2021 the prevalent form of attack was Multi-Vector, closely followed by Volumetric attacks. In 2022, Application vector attacks grew dramatically, by 165%, even as the overall number of attacks went down.

This may be indicative of better defenses being brought to bear. We generally believe that attackers will use the minimum set of techniques that will achieve their goal, whether that is extortion or preventing the operations of their target. In the case of Application vector attacks, this may indicate that it's becoming harder to reliably DDoS a target using solely Protocol or Volumetric means, and that AApplication attacks are more effective.

As a percentage of total traffic (Figure 2), Multi-vector attacks still lead the pack, but only barely. Protocol attacks remained stable at about 10% of observed events, and it appears from our data that more attacks are launched as purely Application attacks, rather than Multi-vector which was the norm before.

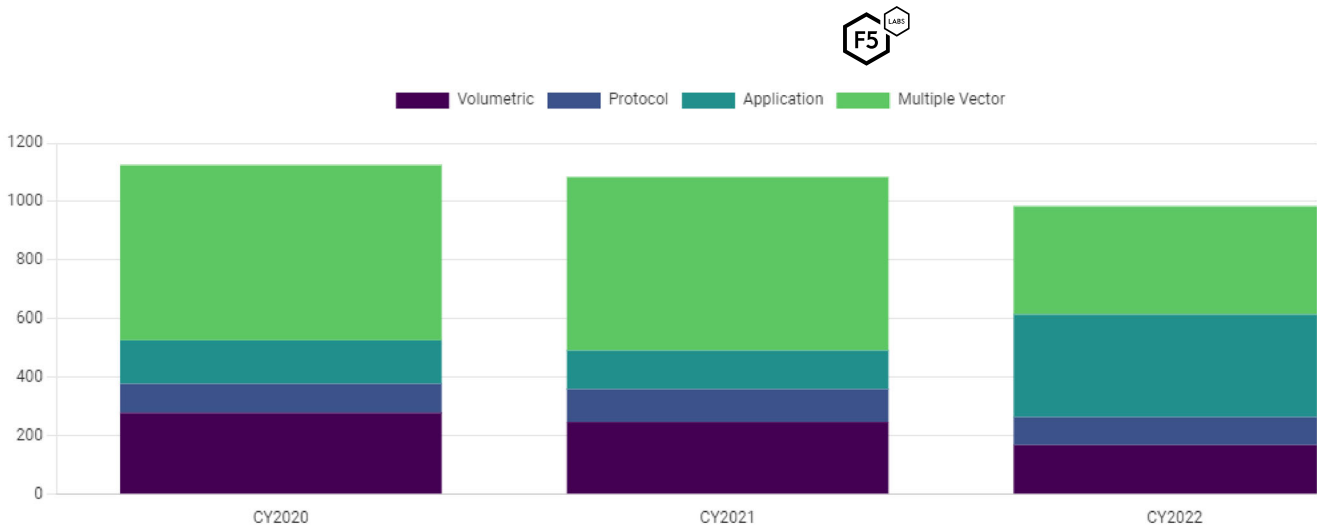


Figure 2 2020-2022 DDoS Attack Category counts. This shows a large increase in the number of Application attacks, with a corresponding reduction in Volumetric and Multiple Vector categories

Trend 3: Peak Bandwidth Back on the Rise

Headlines love to talk about “the largest DDoS ever observed”, and we’ve done that ourselves from time to time, as we did in the 2022 DDoS Attack Trends report. It’s impressive and scary to see attacks in the terabit per second range, since they indicate the immense resources that attackers can bring to bear.

In 2022, the maximum peak bandwidth we observed was 800mbps, down from 1.39tbps the year before, a 42.4% decrease (Figure 3). In 2020 when we observed a peak bandwidth of a mere 253mbps, and so 2022 is still significantly higher, up 216%.

We can take this to mean that attacker capabilities in this area will continue to grow, and that high peak bandwidth attacks are on track to become more prevalent, but it’s worth noting that in our data set, attacks with a peak bandwidth of over 600gbps account for a very small amount of the total events observed. While such attacks can indeed be difficult to defend against, they are far from the most common.

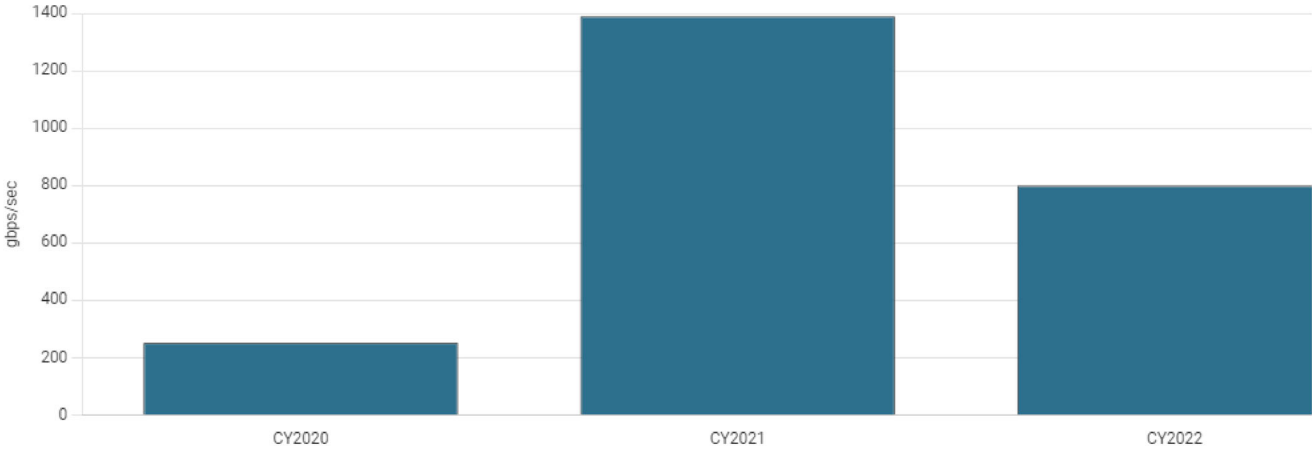


Figure 3 Peak bandwidth in gigabits per second. 2022 rate shows a reduction from 2021, but still significantly up from 2020.

Peak Bandwidth Breakout by Vector

Peak bandwidth alone only tells part of the story.

To dig more deeply, we analyzed the peak bandwidth broken out by the method(s) the attacker used, to find out if some methods trend larger or smaller, and to determine what the “typical” attack might look like in the general case.

To start, we created a scatterplot of the peak bandwidth of all our data points across all three years (Figure 4). Most events are quite small in terms of peak bandwidth, falling under 200gbps. This tells us that while periodic DDoS can be expected to reach 1tbps+ levels, the majority of DDoS that will be seen will be significantly smaller.

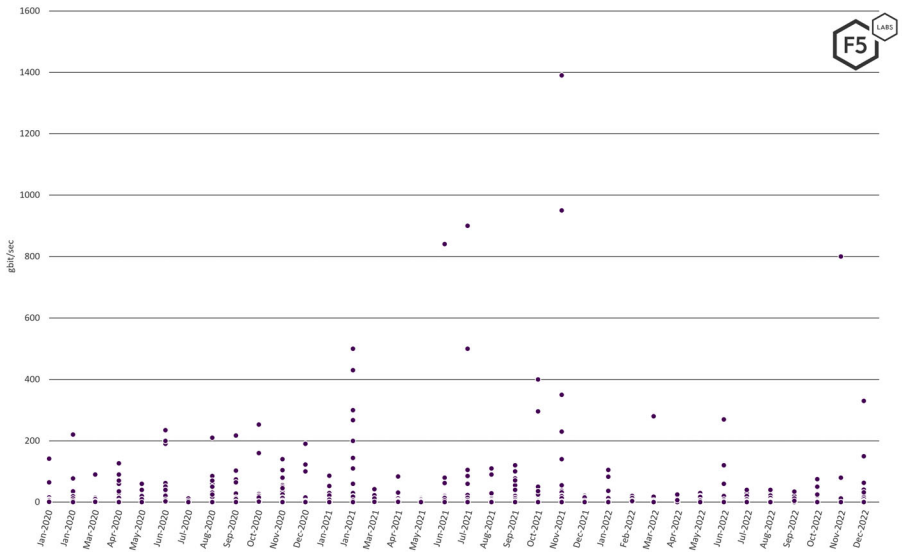


Figure 4 Peak bandwidth per event per month. Most events fall below 200 gigabits/sec

Next, we broke things out by attack method to see how methods related to peak bandwidth (Figure 5).

Please note that to improve readability, we've used a base-10 logarithmic scale for the following charts. We found most events fall between 10mpbs and 1gbps.

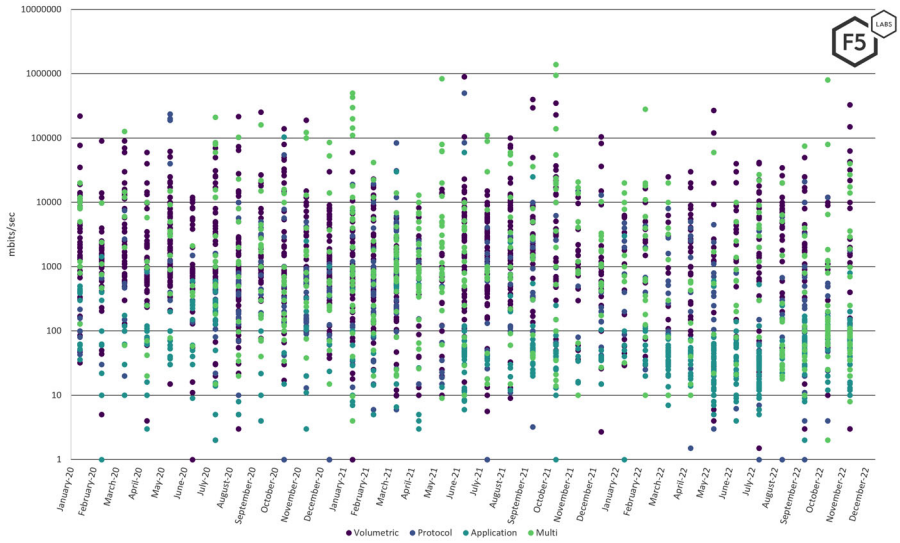


Figure 5 Peak bandwidth by type (logarithmic scale)

Volumetric attacks, as might be expected, trend higher, with most attacks falling between 1gpbs and 10gbps (Figure 6). This makes sense, as volumetric attacks deny service by overwhelming the network bandwidth of the target.

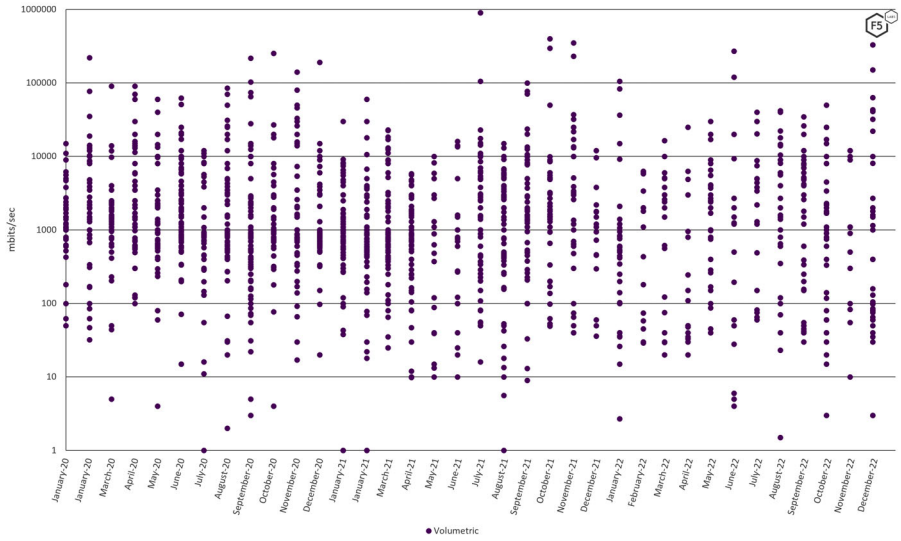


Figure 6 Volumetric peak bandwidth, clustering between 1gpbs and 10 gbps

Protocol attacks fall into a lower band, with most clustered in the 100mbps-1gbps range, with some significant outliers (Figure 7). Since protocol attacks are not attempting to overwhelm network connections, but rather the ability of networking devices to track and direct traffic, less peak bandwidth would be required to achieve an effective DDoS. Nevertheless, the levels observed at times match the highest bandwidth levels used by Volumetric attacks, so in those situations, a 1Tbps+ protocol attack may very well have the same results as a more traditional Volumetric attack.

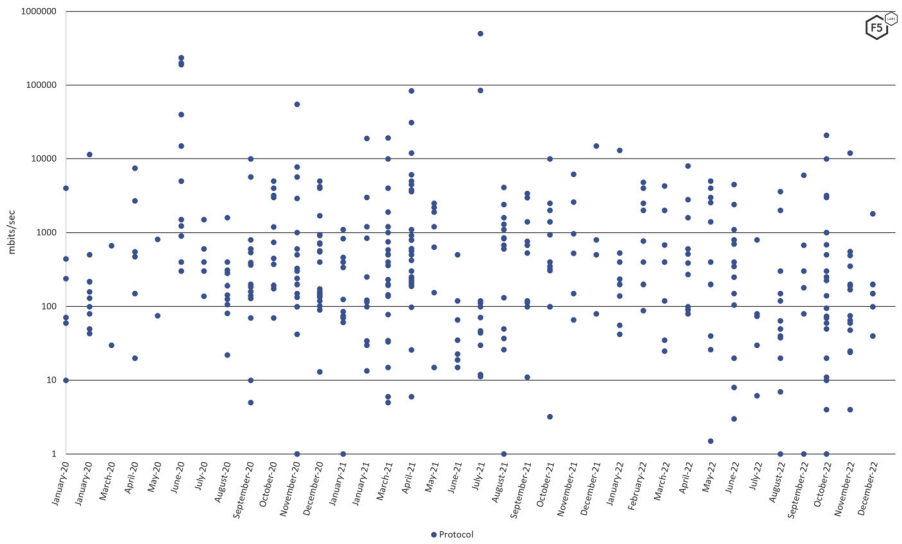


Figure 7 Protocol peak bandwidth, clustering between 100 and 1000 mbps

Application attacks, as might be expected, fall into an even lower range, where the peak bandwidth rarely rises above 1gpbs. But there are outliers here as well, with some reaching peak bandwidths of 100gpbs (Figure 8).

These were primarily DNS request floods in our dataset DNS request floods, which use UDP, require far fewer attacker resources than other Application attacks, such as HTTP GET flooding.

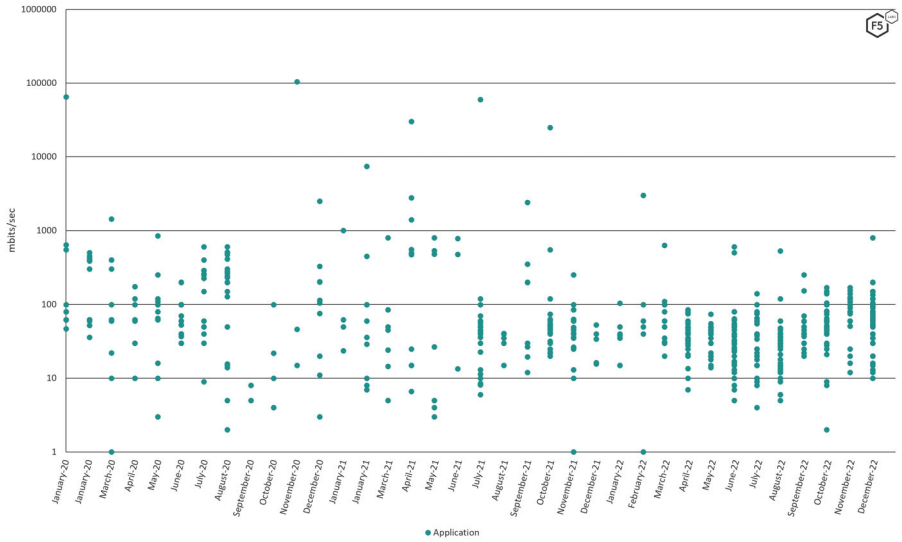


Figure 8 Application peak bandwidth, clustering between 10 and 100 mbps

Finally, Multiple Vector attacks show a much more dispersed range of peak bandwidths, some peaking over the 1 terabit level, and others being quite small (Figure 9).

This range is difficult to explain; it could be possible that less well provisioned attackers attempt volumetric and application type DDoS simultaneously because they lack the resources to achieve a very high throughput purely volumetric attack. In these situations, the multi-vector approach may be a matter of an attacker using what tools they have at their disposal, using as many different ways as possible to achieve their ends, making up for a lack of overall capability.

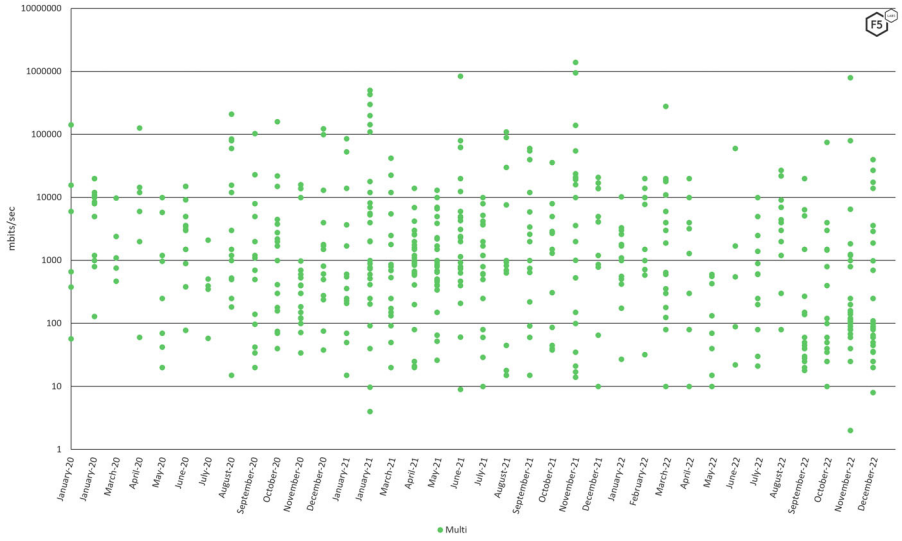


Figure 9 Multi-vector peak bandwidth, clustering between 10mbps and 1,000,000mbits

Tracking DdoS Attack Types Over Time

Another way of visualizing the overall peak bandwidth of each type can be created by taking the monthly rolling mean of peak bandwidth (Figure 10). This is again on a logarithmic scale.

As can be seen, the mean for Application DDoS is currently running at 10-100mbps, Protocol in the 100-1000mbps range, and Volumetric and Multi-vector currently running at 1-10gbps. It is interesting to note that overall, Multi-vector events have led Volumetric more often than not.

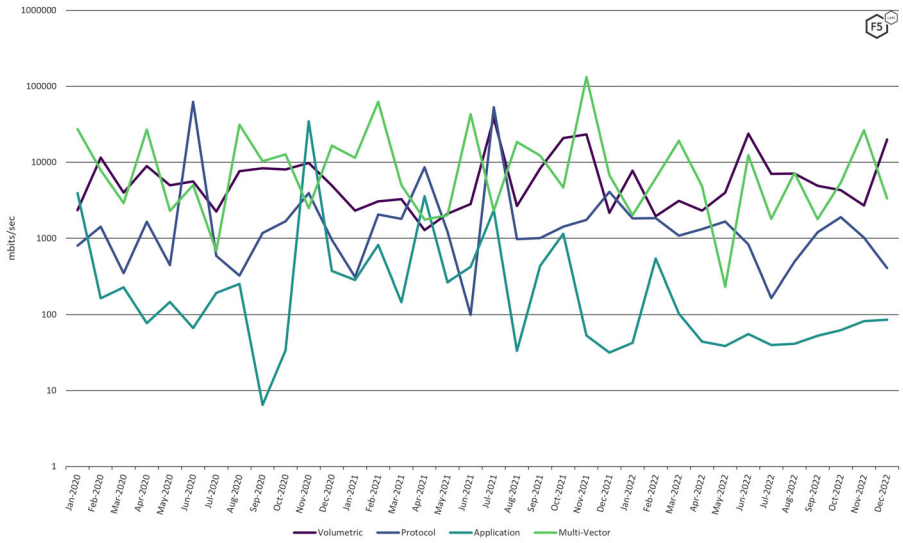


Figure 10 Peak bandwidth over time 2020-2022

DDoS Attacks by Industry Sector

In previous years, we've done a very detailed breakdown of attacks by industry sector, but this time, we decided to talk more generally, rolling up the various categories into "Technology", "Finance, Banking, and Insurance", "Government", "Education", and "Others." (Figure 11)

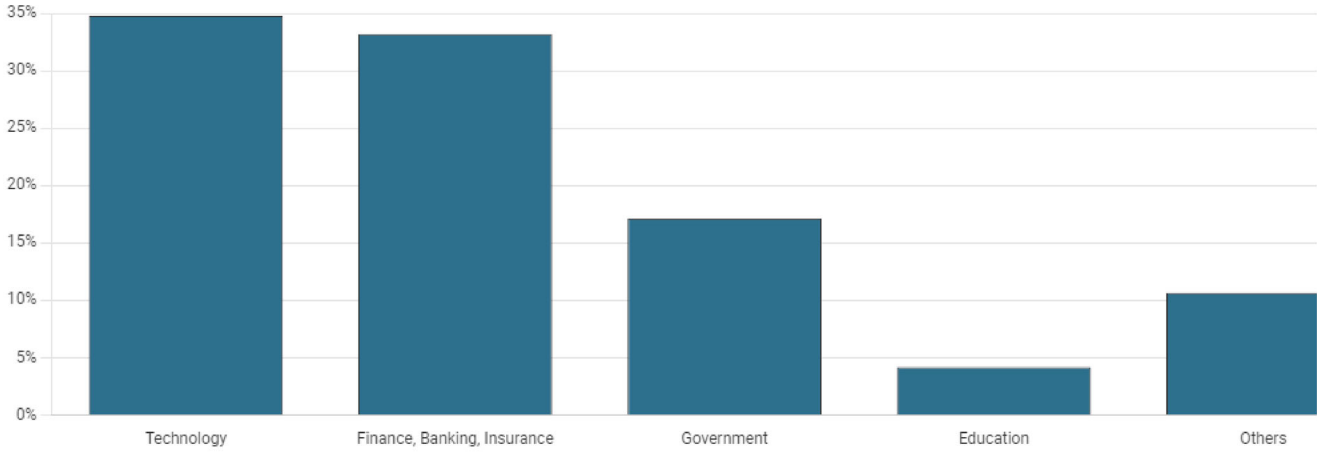


Figure 11 2022 DDoS event counts by targeted industry. Technology and banking are the most targeted.

This allows us to ask a pertinent question – are some industry sectors subject to more of some types of DDoS than others? Do attackers use different methods to attack different industries?

As a percentage of all attacks targeted at organizations within a given class of vertical, the level of Volumetric attacks is relatively consistent, as is the amount of Protocol attacks, outside of Education.

Multi-vector and Application attacks account for most of all attacks and occur with similar regularity in the Technology and Finance/Banking/Insurance sectors (Figure 12).

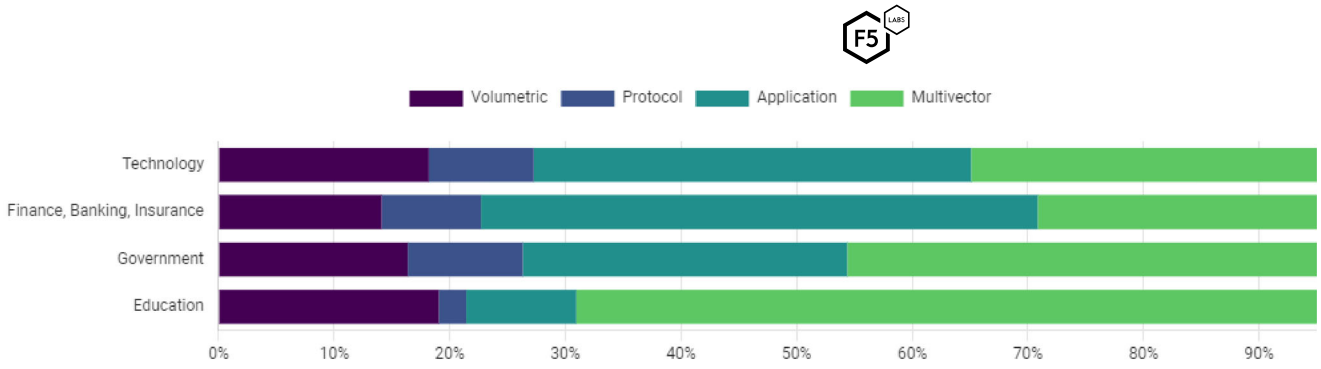


Figure 12 2022 DDoS type by industry. Note the prevalence of Application and Mulit-vector attacks.

Financial and related industries see more DDoS against applications. This may indicate that these industries are well equipped to defend against volumetric and protocol attacks, or that attackers are focused on denying service to the specific applications targeted, or both.

Multi-vector dominates the Education space. We're not entirely clear why that might be, but we do not have as much data on the Education sector as we do for the others, so is probably at least partly a result of sampling bias in our data.

However, the takeaway is clear across all verticals: we must expect Application and Multi-Vector (most often a combination of Application and Volumetric) attacks.

Is Killnet a Sign of Things to Come?

A particularly illustrative example of recent trends is provided by Killnet. Our colleagues in the F5 Distributed Cloud Services SOC have been actively mitigating Killnet DDoS against targeted customers. These attacks have been primarily Application (HTTP/HTTPS) based, and have reached peaks of 120k requests/sec.

As discussed in the recent F5 blog F5 Distributed Cloud Services Stands Up to Emerging L7 DDoS Attacks, Killnet attacks originate from many countries around the world and the attackers have been able to re-tool their approach as new defenses are brought online.

A successful defense against layer 7 (L7) attacks, also known as Application layer attacks such as seen here is far more complex than defending against a simple volumetric attack. L7 attack traffic is harder to identify, as it often appears quite similar to legitimate traffic, and care must be taken to not accidentally deny access to legitimate users.

It's worth noting that of the Application attacks we have in our dataset, the vast majority were DNS request floods – 93.4% in fact. These certainly can be devastating. DNS is a critical piece of infrastructure, and flooding DNS servers with queries for non-existent subdomains, can cause a great deal of reduction in service, often preventing genuine customers from being able to reach their desired application. This is especially true when the DNS server in question signs their response, as is the case with DNSSEC, which adds additional work

for each request. However, Killnet may be showing us what things will be like in the future, with an increased attention paid to web application DDoS. Time will tell.

Conclusions

Based on the above analysis, we can expect to see a continuing trend of increases in DDoS events and the peak bandwidth they will exbibit. Specifically, attacks leveraging Application vectors are becoming more and more common, with the second most common combination being Multi-vector approaches. All industries should expect these trends, but larger companies whose business relies on the availability of web applications should pay special attention to web-based denial of service.

While multi-terabit attacks will continue to occur from time to time, the majority of DDoS use significantly less bandwidth. However, given the wide range of bandwidths observed, even the most frequently observed bandwidths may be well beyond the ability of on-premises solutions to defend against.

Recommendations

At this point, we feel that using scrubbing services or provider-level defenses against DDoS are necessary for any organization who is serious about defending against these attacks. These can provide defenses that would be completely beyond the capabilities of an individual organization, especially for 1+ Terabit attacks. As a side benefit, these systems will also defend against the much less intense, but much more common, levels of DDoS that most organizations can expect day-to-day. There really isn't any reason to try to do it yourself; the economies of scale that scrubbing providers can bring make it a far more effective, and cost-effective, approach.

This frees up the individual organization to focus on attacks that target their specific applications, which is where, according to our data, attackers are shifting their attention. Automated attacks, even when not intentional DDoS

(for example, scraper bots, reseller bots) are not necessarily going to be caught by scrubbing services, and it makes sense to apply defenses against these attacks at a more granular and customized level.

Authors & Contributors

Malcolm Heath (Author)
Sr. Threat Researcher
About Malcolm All Articles

Sander Vinberg (Contributor)
Threat Research Evangelist, F5 Labs
About Sander All Articles

Footnotes

TAGS: DDoS Attacks • SSL-TLS renegotiation • Threats • Hacktivism • DNS reflection • Killnet • DNS flood • SYN, UDP, and HTTP floods • Attack Campaign • Heavy URL • Network Tier • DNS amplification • UDP flood • Protocol Abuse • DNS Tier • TLS Tier • SYN flood • HTTP flood • Tofsee Botnet • Services Tier