imperva

2021 REPORT

Global DDoS Threat Landscape Report

Contents

Executive Summary

Distributed denial of service (DDoS) attacks have been a significant feature of the cyber threat landscape over the past two decades. As the 2021 Imperva 2021 Global DDoS Threat Landscape Report shows, attacks are constantly evolving in size, volume, frequency and complexity. What doesn't change is the attackers' focus on critical infrastructure. Not only is the number of DDoS attacks per month increasing - attacks have increased four-fold - but volume and packets are also on the rise since 2020, at 2X and 3X respectively.

While we were compiling this report, Imperva mitigated its largest DDoS attack to date, with a throughput of 1.02 terabits per second (Tbps) and 155 million packets per second (Mpps). Previously, Imperva had stopped attacks in which highs were 646 gigabits per second (Gbps) and 936 Gbps in August and September 2020, respectively. Although those attacks took place outside the scope of this report (the first half of 2021), they serve to underline a clear trend towards shorter, higher volume attacks, where the average attack duration is just six minutes.

Coupled with a rise in the use of Transmission Control Protocol (TCP), it's clear that attackers understand that organisations with low or no defenses are easy targets. For those without always-on defenses in place, shorter attacks allow attackers to create maximum disruption before mitigation can kick in. When attackers take this "rinse and repeat" approach, it's harder for organizations to mitigate and manage attacks.

As far as targeted industries are concerned, the focus of the attackers in 2021 are the Computing and IT, Corporate Business and Financial Services sectors.

Finally, it's notable that, in the first half of 2021 (H1 2021), every day was a good day for DDoS attackers: attack volumes were consistently high every day of the week.

Highlights

Big, bigger, biggest
July 2021 saw Imperva mitigate its biggest DDoS attack to date, with a throughput of 1.02 terabits per second (Tbps) and 155 million packets per second (Mpps).

The only way is up
The number of DDoS attacks per month is up; attacks are up 4X, volume of attacks has increased 2X and the number of packets has increased 3X over 2020 numbers.

Short, sharp and persistent
Attack duration is going down, but packets and volume are increasing. Shorter attacks are dangerous as they may be a distraction tactic as part of a wider multi-vector attack. Legacy DDoS solutions are often configured to ignore this level of activity, giving attackers the opportunity to stay under the radar and scope out larger attacks.

Ransom DDoS attacks are back
Ransom threats are on the rise. Imperva Research Labs have monitored threats against several of our customers where extortionists have demanded payment in BitCoin to prevent a DDoS attack. The attack patterns this year are very similar to those seen in 2020.

HIGHLIGHTS

2021 biggest DDoS attack to date

DDoS attacks per month are up

Attacks are up 4X

Volume of attacks has increased 2X

Number of packets up 3X over 2020 numbers

Ransom DDoS attacks are on the rise

Financial Services was the focus of over 22% of application layer DDoS attacks

Computing and IT is the most targeted industry

The Computing and IT industry accounted for 29% of all application layer, or layer 7 (L7) attacks. Financial services was the focus of over 22% of application layer DDoS attacks.

Network DDoS attackers love Fridays

Friday was the most popular day of the week for network DDoS attacks, but there's an overall upward trend of attacks across the week compared to 2020, when Sunday was the most popular day.

TCP attacks are on the rise

User Datagram Protocol (UDP) reflection/amplification is still the main protocol used by attackers but TCP attacks have increased significantly. Organizations that lack DDoS defenses are easily taken out by low volume TCP SYN attacks, making them the perfect weapon of choice for attackers.

SYN floods have increased in volume

SYN and large SYN floods in the first half of 2021 had much larger volume compared to 2020. Large SYN attacks were seen mainly on websites and less often on networks.

DDoS attacks: Low barrier to entry, high capacity for damage

DDoS attacks have been a significant feature of the threat landscape. What began largely as a form of protest and sabotage has evolved into big business for cybercriminals. Today, anyone can launch a DDoS attack for the price of a good cup of coffee, and $100 is enough to cripple a network.

As this year's report shows, DDoS attacks are constantly evolving in size, volume, frequency and complexity. What doesn't change is the attackers' focus: the infrastructure their targets depend on most. That could be customer-facing applications, cloud services, network infrastructure or an ISP. As organizations continue to pursue digital transformation, the technologies that drive this - cloud services, mobile networks and IoT devices - are becoming targets. New vectors are being weaponized all the time.

[1] Gartner, The Cost of Downtime, Published 16 July, 2014, Andrew Lerner.

[2] Imperva Global DDoS Threat Landscape Report, 2019

Network DDoS Trends

Network layer attacks: Short, sharp and persistent

When DDoS attacks hit, websites and online services attract most of the attention. But DDoS attacks can be launched against other infrastructure elements like routers, firewalls, load balancers and domain name servers (DNS). A network outage doesn't just cause IT problems - call centers, customer service and order fulfillment can all take a massive hit.

Imperva Research Labs found an ongoing trend of short, sharp, persistent attacks during the first half of 2021. These typically overwhelm hybrid cloud and on-premises solutions, causing maximum damage before backup cloud mitigation can start. By continually circling back to hit again, attackers can leave networks "punch drunk". These shorter, more intense hits are difficult to mitigate, unless you have always-on protection. By the time you notice the attack, it has stopped. Problem is, you don't know when it's going to start again.

It's possible that these attacks are part of an increasing trend towards Ransom DDoS, where attackers claiming association with notorious threat actors such as Cozy Bear and Lazarus launch a few proof of concept hits to scare victims into paying up. Equally, the shorter, more persistent attacks could reflect an awareness among attackers that many organizations continue to rely on mitigation services that take longer to react than the attack itself lasts, rendering them essentially useless in the face of repeated short hits. By cutting off the network's ability to communicate with the outside world, attackers not only cause a denial of service, but prevent mitigation appliances from activating the cloud scrubbing platform.

The high cost of a network DDoS attack

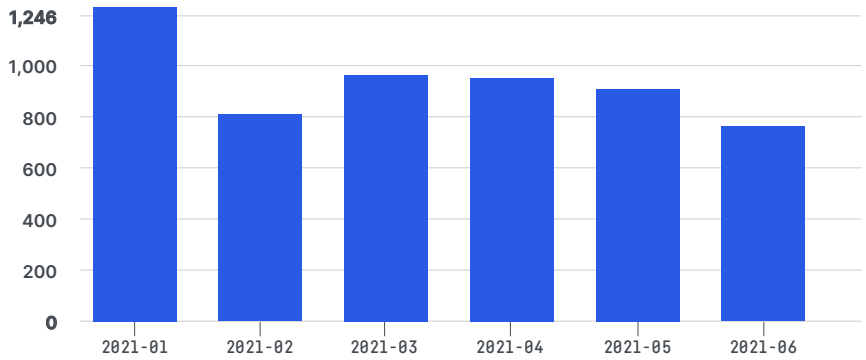
When a multinational gaming company received a ransom note threatening a DDoS attack in 2020, they decided to ignore it. Soon afterwards, they began noticing proxy errors from their website and couldn't reach their origin servers. Further investigation revealed that they weren't receiving any packets at all from their servers. When they contacted their ISP, it emerged that they had been cut off as "noisy neighbours" - i.e. the attack on their site was impacting resources for other customers, so the ISP "blackholed" them to protect others. The cost? Twelve hours of downtime, 39 engineers on call to mitigate, $42k for a one-hour website outage and a call center meltdown that saw a loss of productivity for 39 agents for 12 hours. Total cost = $600k. When you consider that down time can cost as much as $300k an hour, this could have been a lot worse.

Here's what Imperva Research Labs has learned about network layer attacks in 2021.

Number of DDoS attacks per month, in the first half of 2021

Overall, there were 5,591 network layer (Layers 3-4) DDoS attacks in the first half of 2021.

January started off with a bang, before a slight dip in February followed by a more or less consistent 800-900 attacks per month over the remaining period.

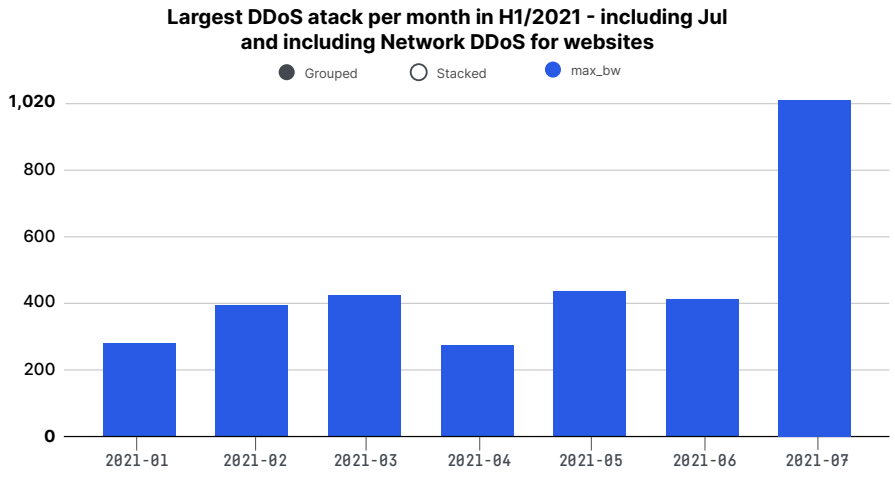


Largest DDoS attack per month in the first half of 2021

As the true measure of attack intensity, packets per second matter far more than the amount of bandwidth involved - this is what's difficult to block and recover from. March, May and June all saw attacks that peaked in excess of 400 Gbps, with the lowest still recording a max of 263 Gbps.

When you consider that even a couple of tens of thousands of packets per second can overwhelm your systems, these numbers are massive. Even 1 Gbps is enough to take most organizations offline.

Factor in the massive attack mitigated by Imperva in July 2021, and you can see how it dwarfs the network and website DDoS attacks recorded in the earlier half of 2021.



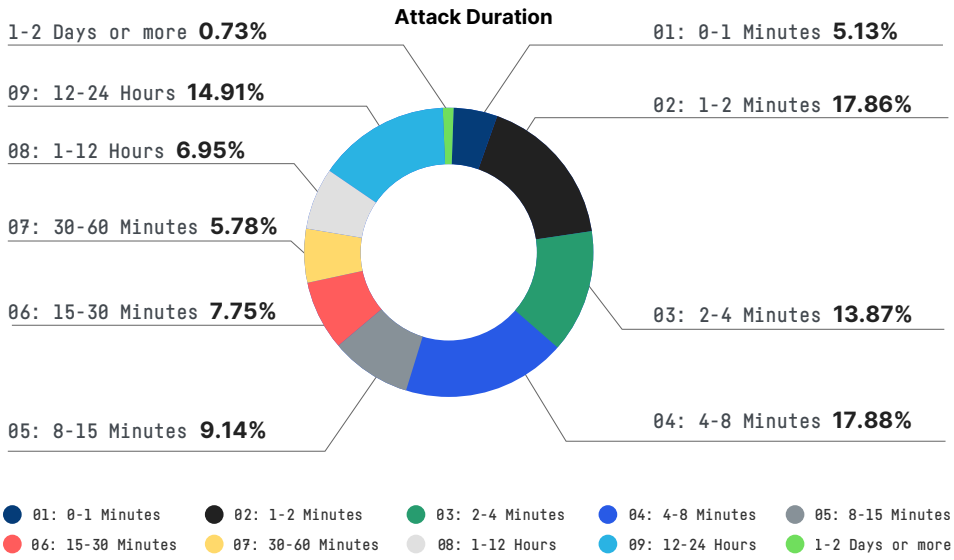
Attack duration

The median duration of a DDoS attack in H1 2021 was 6.1 minutes - short enough to cause trouble but too short to mitigate for any organization with insufficient protection in place. This trend towards even more unpredictability underlines the importance of always-on protection and rapid mitigation. If the attackers are going to keep circling back in short bursts, always-on is the only genuinely effective strategy.

Shorter, stealthy DDoS attacks are often used as a "smokescreen" to disrupt and distract network teams while threat actors infiltrate the wider network to exfiltrate data or install malware. These shorter attacks can remain under the radar because organizations using outdated or unsophisticated DDoS mitigation technology often configure detection thresholds that ignore this lower level of activity. While IT staff are preoccupied.

with getting a firewall or intrusion prevention system back online, the attackers are busy installing malware, accessing other parts of the network or simply perfecting their techniques.

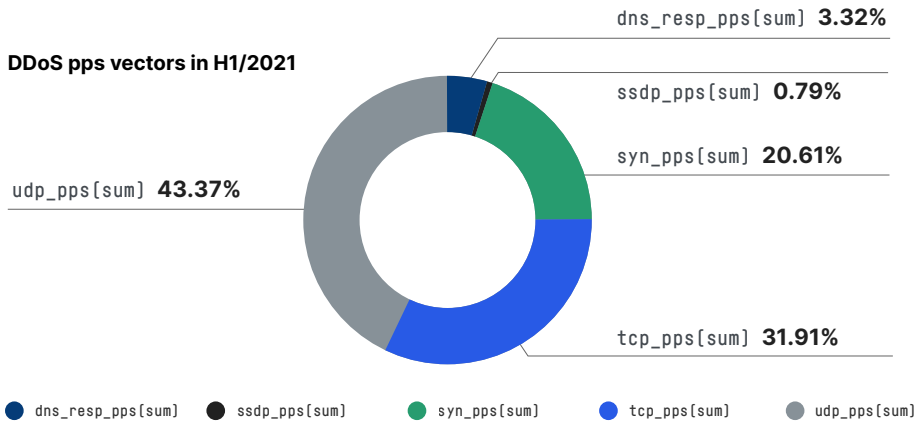
Imperva Research Labs found that while a very small (0.73%) number of attacks lasted as long as 1-2 days or more, more than a third lasted 1-4 minutes, with just over a quarter lasting 4-15 minutes.This trend underlines the need for swift mitigation - essentially, within seconds. Reaction times that take longer to muster than the attack lasts offer no defense.



Attack Trends

Packet-based DDoS vectors

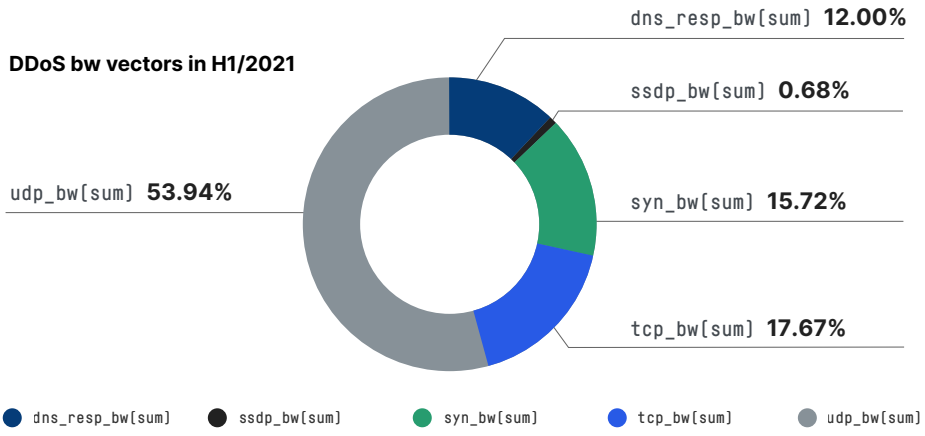
As in our previous report, UDP was the most popular protocol for DDoS, probably because it's easy to spoof, is used in all amplification attacks and is widely used in high-risk industries such as gambling and gaming. What changed between 2020 and 2021 is the use of TCP: soaring from just over 10% to almost 32%.



Bandwidth-based DDoS vectors

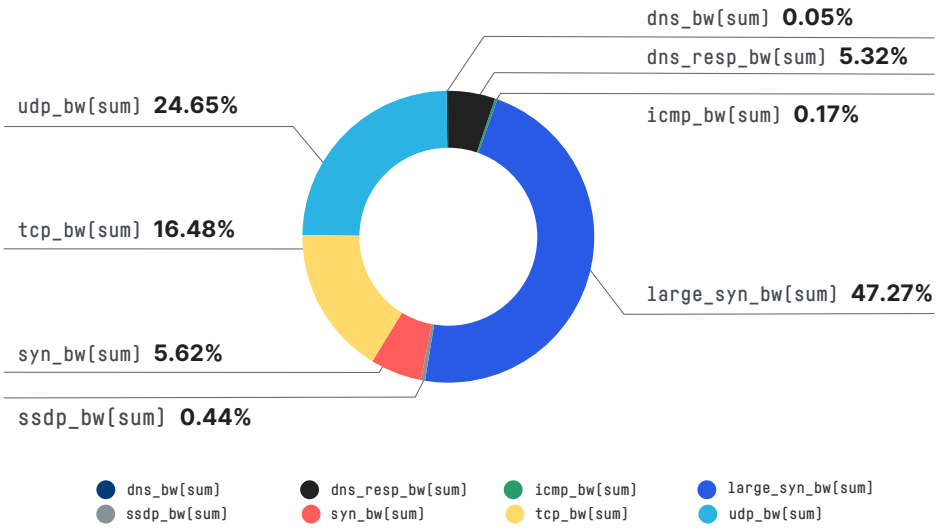
DDoS bandwidth attacks flood networks with large volumes of spurious data designed to consume so much bandwidth that the network is congested and starts dropping packets - affecting legitimate traffic. Imperva Research Labs data shows that, although UDP remains the most popular protocol for these attacks in the first half of 2021, it has dropped from 78% to 54%, with the gap being filled by a significant growth in TCP and SYN.

Attacks on TCP increased significantly, from 4% in H1 2020 to 18% in the same period of 2021.



When you include websites alongside network DDoS attacks, large SYN accounts for almost half of the vectors.

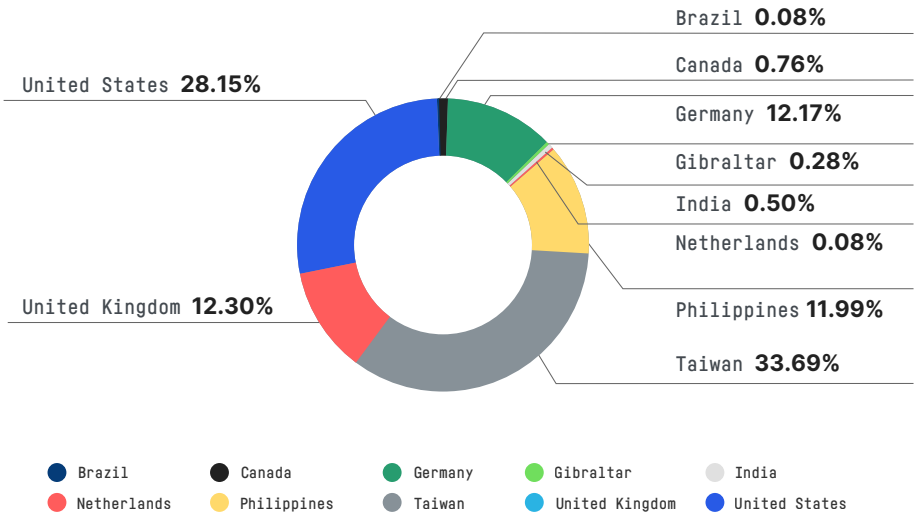
DDoS bw vectors in H1/2021- more vectors BGP + websites



Top attacked geographies

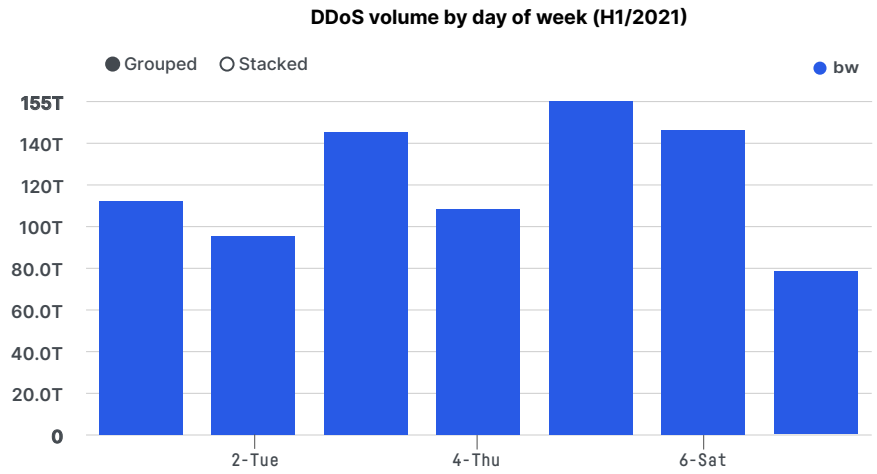
In the first half of 2020, the top attacked country for network DDoS was the Philippines, followed closely by Taiwan. One year later, Taiwan is the leading target (33.6%); up from 31% the previous year. Meanwhile, the USA is a close second (28.15%); up 10 percentage points from the year prior. The United Kingdom and Germany effectively sharing third place.

Attacked Countries in H1/2021 - Top 10



Every day is a good day for DDoS attackers

At a global level, Sunday had the highest daily attack volumes in 2020. Fast forward to 2021, and not only are volumes consistently higher but Friday is the biggest day, followed very closely by Wednesday and Saturday. Attacking on Fridays provides a good opportunity to catch organizations focused on gaming or gambling off guard, causing maximum disruption - and hitting IT teams with the prospect of a weekend of crisis management.



Whatever way you want to look at it, from volume to number of attacks per day, every day is a good day for DDoS attackers.

Application layer DDoS attacks: Punching well above their weight

Application layer (Layer 7) attacks target Internet-facing critical business applications. They exploit weaknesses and vulnerabilities in the applications themselves. Because this is the closest layer to end users, it offers the widest threat surface to attackers.

Measured in requests per second (RPS - the number of requests made of an application) Layer 7 attacks are highly effective because they consume both network and server resources. It doesn't take a lot of bandwidth to completely paralyze the target, meaning attackers can do a lot of damage, even with limited resources. Defending against application layer attacks can be tricky. You need to be able to distinguish between attack traffic and normal traffic, and this can be difficult when every bot in a botnet is making network requests that look legitimate.

Application DDoS Attacks In 2021

Maximum Requests per Second Blocked

In 2020, just under a third of all application layer attacks mitigated by Imperva were under 1,000 RPS (29.96%). In 2021, it's trending up to 43%.

Compared to the first half of 2020, 2021 saw a decrease in the maximum size of requests per second mitigated by Imperva: 258,898 rps, down from 386,751 the previous year.

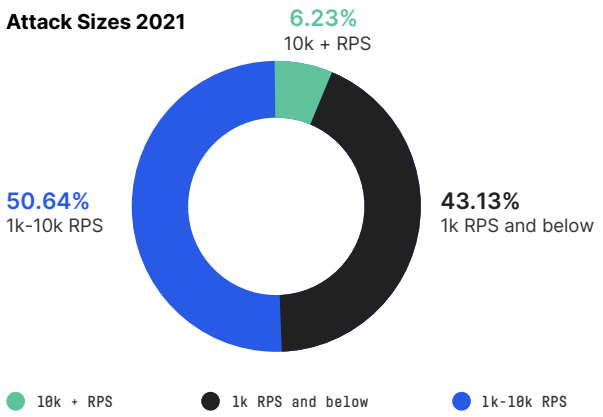
The high cost of a network DDoS attack

In July 2020, Imperva recorded a massive application layer DDoS attack on a Chinese gambling site. Originating from 851 different source IPs, the attack lasted less than 10 minutes, during which time it reached an incredible 689,000 requests per second (RPS) at its peak - an intensity that would have quickly overwhelmed the site's servers, bringing it to a grinding halt.

The attack was unprecedented for 2020 but, as Imperva Research Labs noted at the time, they were part of a trend that year towards larger and longer application attacks. During the month of July 2020 alone, Imperva observed 12 major application attacks with a volume in excess of 150,000 RPS.

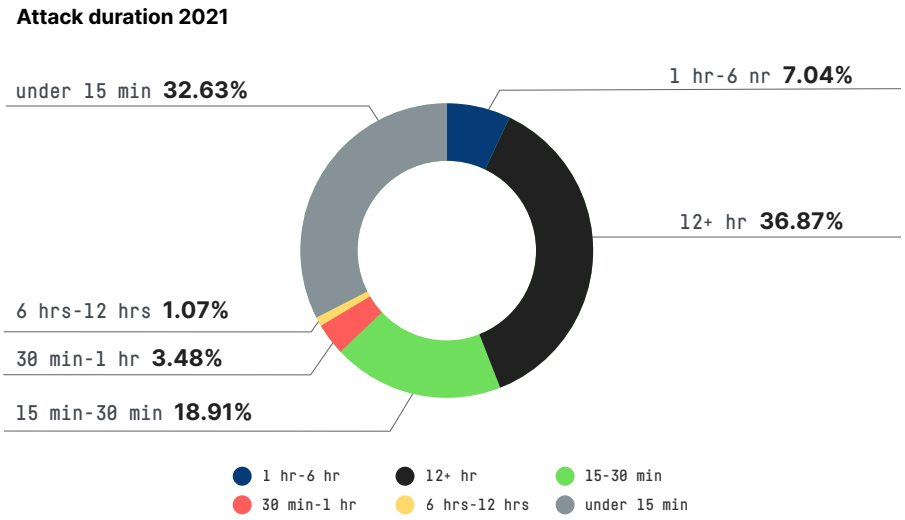
In keeping with the overall trend for network attacks, application layer attack sizes in H1 2021 were lower than in the same period last year. The number of attacks hitting harder than 10,000 rps decreased from just under 13% in 2020 to 6.32% in 2021; almost 51% of all attacks were between 1k-10k rps, a small decrease from 2020 (57.32%).

Relatively low-budget, lower-skilled players are making the most of a wide variety of 'stresser' services to rent out and launch attacks. Higher throughput attacks are usually the realm of more sophisticated, expert attackers with access to their own botnets and resources. The takeaway here is even low-RPS attacks have the capacity to bring down application components or the supporting databases, by finding resource-intensive entry points or services such as search functions.



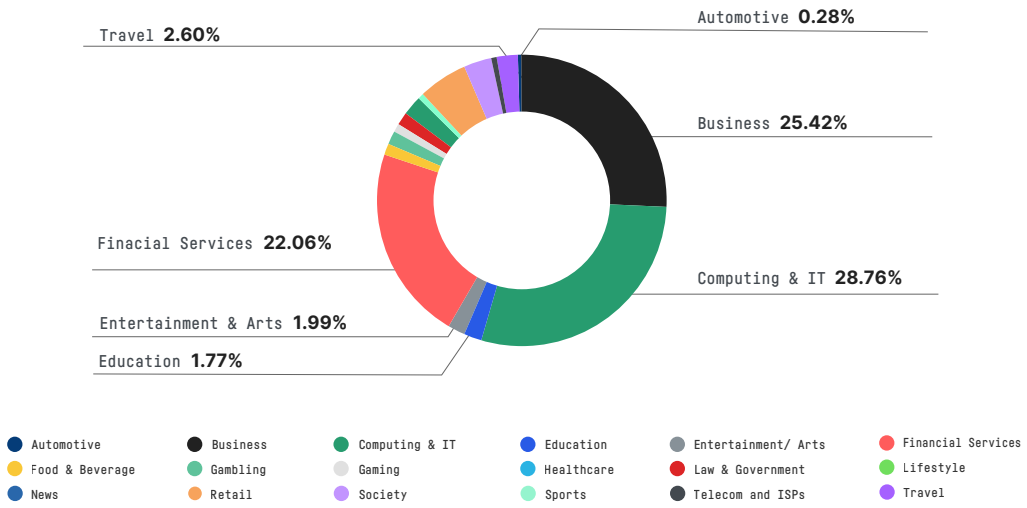
Attack duration

Just over a third of application layer DDoS attacks lasted more than 12 hours - and just over a third lasted less than 15 minutes.



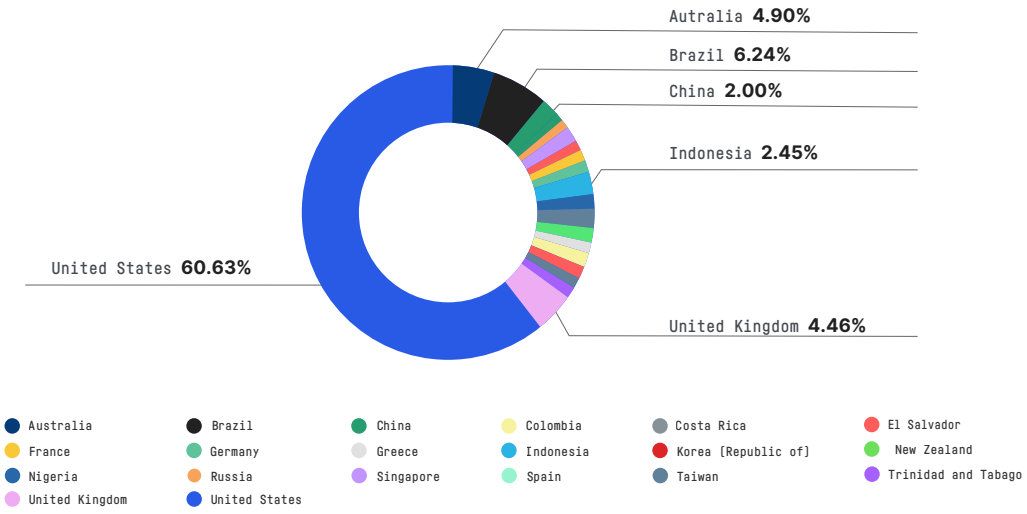
Most attacked industries

Computing and IT organizations accounted for almost 30% of all application layer attacks mitigated by Imperva in the first half of 2021 followed closely by corporate business accounts (25%) and financial services accounting for 22% of all application layer DDoS attacks.



Most targeted countries

As monitored by Imperva Research Labs, the United States of America was by far the most targeted country for application layer DDoS attacks in H1 2021 at 60% of the total. Runner-up Brazil accounted for 6.24%.



Finally

The trend towards shorter and sharper attacks that Imperva Research Labs observed last year continues for network layer DDoS. This reality underlines a clear need for always-on DDoS protection, along with faster reflexes for time-to-mitigation.

When DDoS attackers are capable of attacking at will, there's little comfort in the trend towards shorter attacks; the level of persistence can't be ignored. In this respect, the largest attack ever mitigated by Imperva, in July 2021, is informative - as it ramped up to an eye-watering 674 Gbps burst in under five seconds. In a case like this, where the first wave of the attack involved a 90 second burst of a large SYN flood, being able to start mitigation in seconds is vital. This type of attack would be impossible to mitigate with an on-premises or hybrid DDoS approach, where upstream connectivity would be totally overwhelmed.

To learn more about Imperva DDoS Protection - and find out what makes Imperva a Leader in the Forrester Wave™ : DDoS Mitigation Solutions for Q1 2021, visit imperva.com