imperva

Report

DDoS Threat Landscape Report Q2 2022

Table of Contents

Executive Summary

Today's DDoS attacks are reaching new records in rates, frequency, and complexity

Imperva observed a new trend in the second quarter of 2022 when we detected and mitigated record-breaking DDoS attacks that reached new records in rates, frequency, and complexity on multiple levels. Such attacks emphasize the importance of early and proactive mitigation, and not just at the application layer.

At the onset of Q2, an attack at the extremely high rate of 10M Rps occurred using only **12K IPs**, and as the quarter ended, a single attack of **25.3 billion requests** measuring **3.9M Rps** set new records. Notably, in both events, the attackers used HTTP pipelining and HTTP multiplexing, techniques that are becoming increasingly common. The attacks also maintained the high rates for several hours, rather than only several seconds to minutes, which was the trend previously. This new trend suggests that today's DDoS attacks are more sophisticated and reach new records often, maintaining high rates of attacks for a longer duration. The new trend also means that it is more important than ever to block attacks at their earliest onset, with an efficient mitigation solution that stops DDoS attacks within seconds.

Also in Q2, the number of application-layer attacks increased overall compared to Q2 2021, and while network-layer attacks decreased compared to Q1, **the number of major attacks (over 500 Gbps) rose by 287%**, suggesting that attackers are focusing their efforts on stronger attacks than ever before.

DDoS attacks are also being leveraged by hacktivists to disrupt government websites and operations. Attacks on both Russia and Ukraine sites were up this quarter compared to Q1, and Imperva observed a clear increase in the size of attacks on Israeli websites as we mitigated attacks on large Israeli transportation, telecommunications, and government sites.

Finally, repeat attacks were up 5% compared to Q1 in the application layer, and in the network layer, **91% of DDoS targets were attacked again within just 24 hours**.

HIGHLIGHTS

Imperva mitigated a record-breaking attack **of 25.3 billion requests**

Imperva detected a **10 M rps** DDoS attack

60% of all application-layer DDoS attacks lasted **15+ minutes**, and **21%** of all network-layer attacks lasted **1+ hours**

55% of sites hit by layer 7 DDoS attacks in Q2 were attacked again

91% of network-layer DDoS targets were attacked again within **24 hours**

25% of gambling sites were attacked in the final month of Q2

Q2 Highlights

Imperva mitigated a Layer 7 record-breaking attack of 3.9M Rps

A single attack toward the end of Q2 broke Imperva records in terms of the rate at 3.9M Rps mitigated at the application level, with total requests at 25.3 billion in less than 5 hours while maintaining the high rates. Because of Imperva's industry-leading mitigation rate, we were able to shut down the attack, preventing it from growing much larger than the initial rate of 3.9M Rps.

This attack was launched from a massive botnet of 48,480 different IPs. The most common client in this attack was classified as Node.js. A myriad of devices, from routers to web cams to compromised servers, took part in the attack.

During one week of attacks, sources of the attacks on this specific site came from:

Imperva detected a 10M Rps DDoS attack

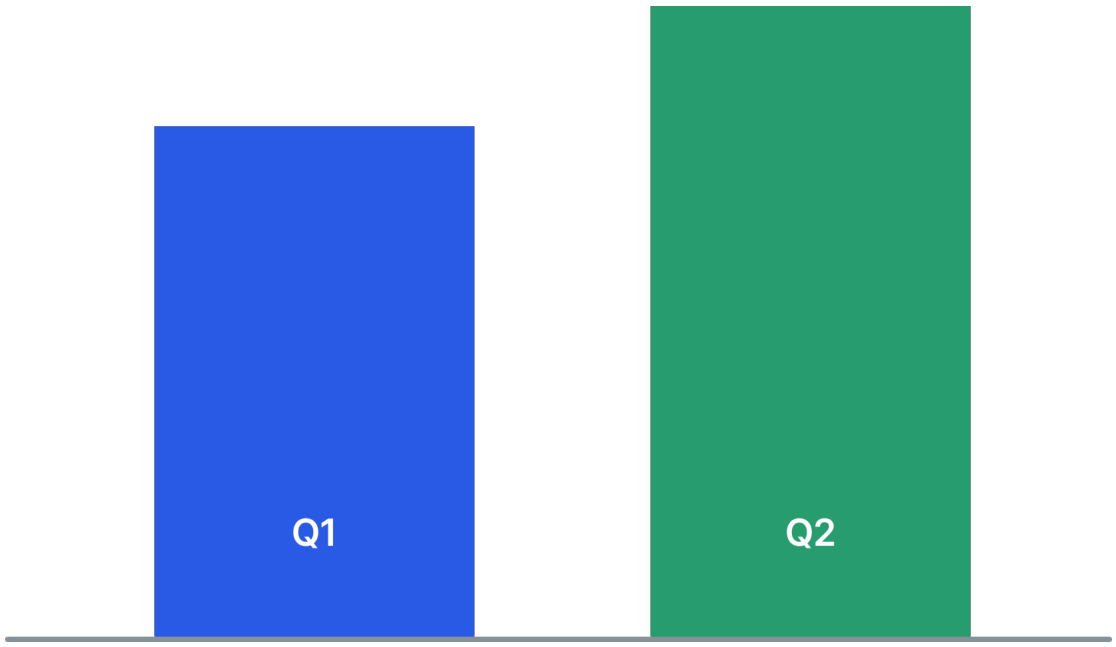
In an earlier record-breaking attack at the beginning of Q2, the highest rate was detected when hackers using HTTP pipelining reached **10M Rps** in a DDoS attack using **only 12K IPs!** Million-plus-request-per-second attacks are nothing new, but until recently, they lasted only for a few minutes at most. Now, though, they appear to be lasting for more than four hours while maintaining extremely high rates. Today's attacks are evolving beyond a few million Rps, reaching new records in rates, frequency, and complexity.

DDoS attacks continue to disrupt during geopolitical unrest

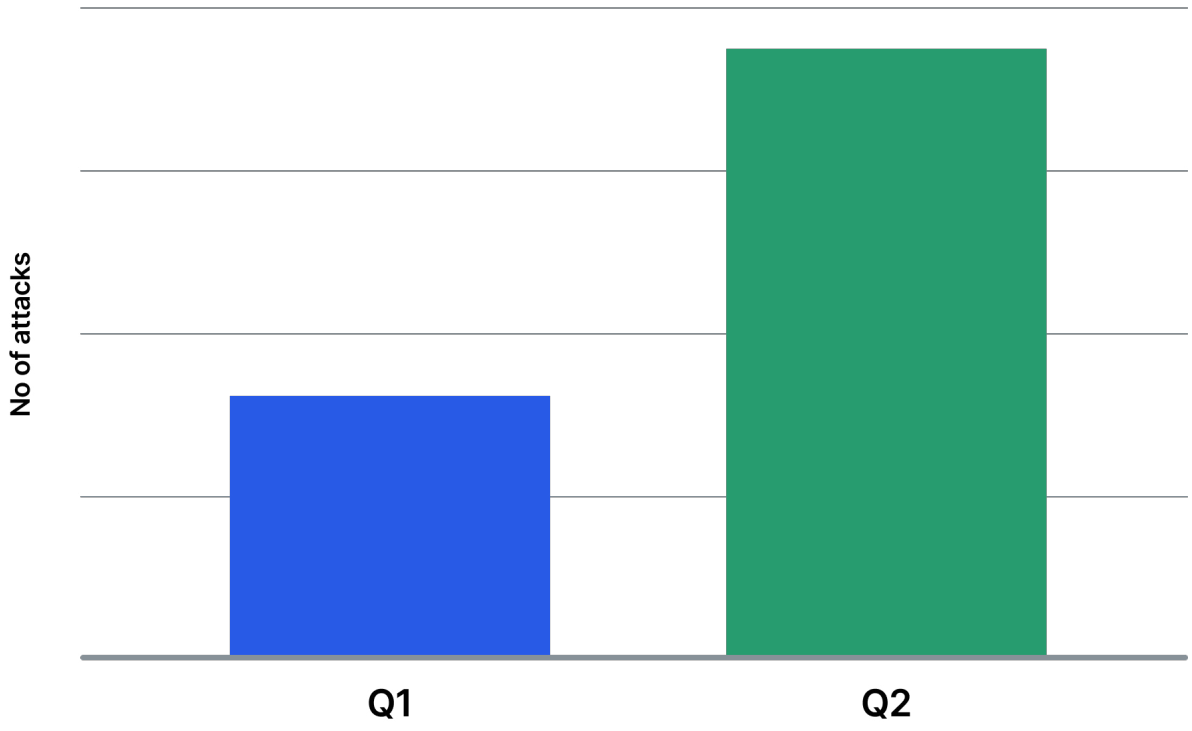
This quarter, application layer DDoS attacks on Russia and Ukraine by hacktivist groups continue to disrupt large websites and operations in both countries.

The number of Layer 7 DDoS attacks on both Russian and Ukrainian sites increased in Q2.

Application Layer DDoS attacks on Russian Sites Q1 vs Q2

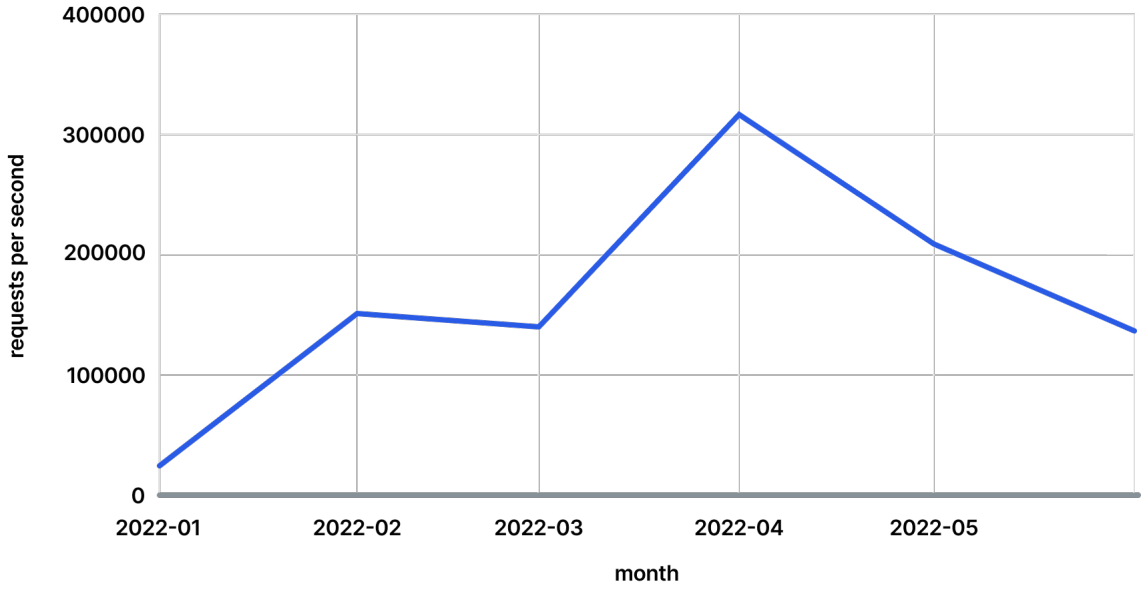


Application Layer DDoS attacks on Ukrainian sites Q1 vs Q2



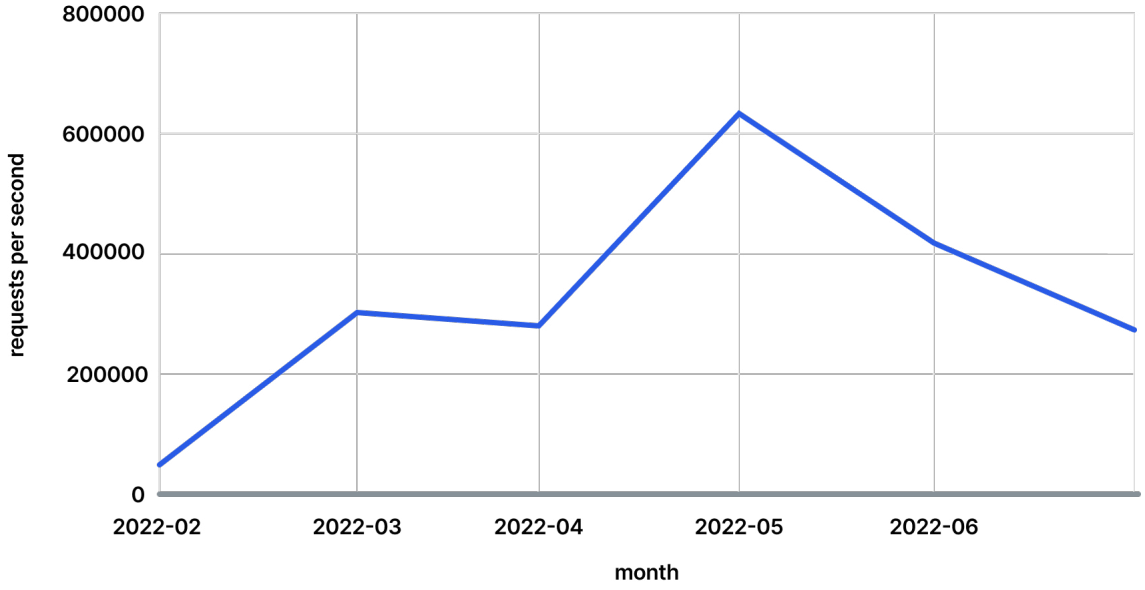
The rate (Rps) of Layer 7 DDoS attacks on Russian sites also increased.

Attacks on Russian SItes in Rps



Meanwhile, in the Middle East, a number of DDoS threats and attacks, possibly linked to the ALtahrea Team and other Iraq and pro-Iranian threat groups, have been carried out on Israeli websites during Q2. The attacks included the Israel Airports Authority[1] and reached as far as the UK's Port of London Authority[2]. Imperva mitigated attacks on large transportation sites, telecommunication sites, and government sites as part of these attacks.

Application Layer DDoS Attacks (by Rps) on Israeli sites



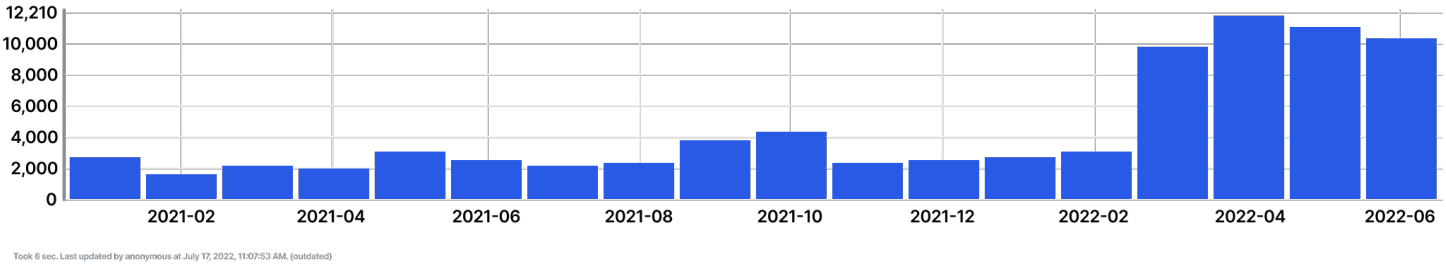
Attacks on Israeli websites by month increased in size (Rps)

1_https://www.databreaches.net/report-pro-iran-hackers-target-israel-airports-authority-website-israeli-portal-also-hit/
2_ https://infosectoday.com/cybersecurity/pro-iran-group-altahrea-hits-port-of-london-website-by-ddos-attack/

Application-layer DDoS Attacks

3X increase in the number of Layer 7 attacks

There was a 3X increase in the number of attacks in Layer 7 in Q2 compared to Q1. This is further evidence that DDoS attacks are growing larger in number, size, and rate quarter by quarter in 2022 thus far.

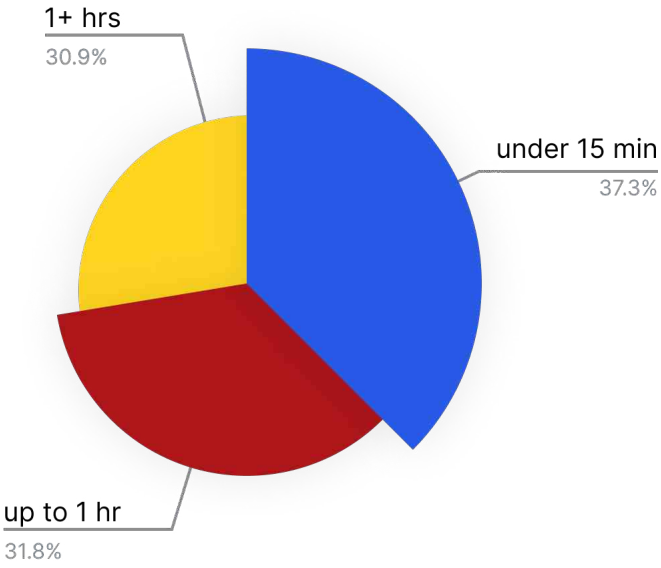


Number of attacks since January 2021

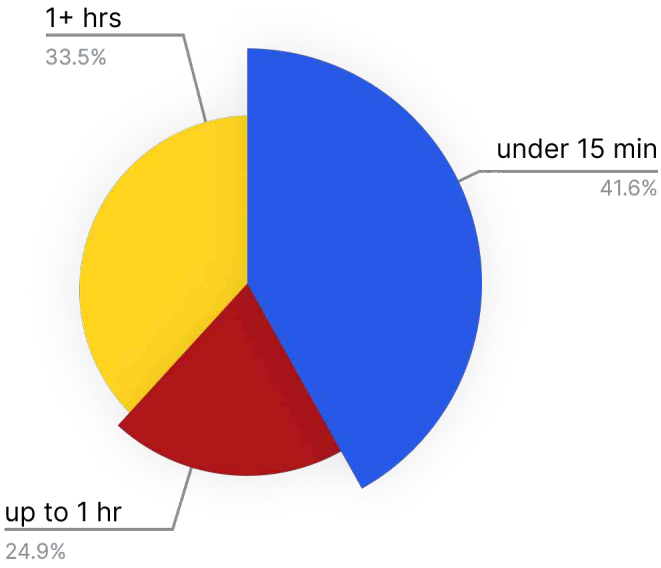
Attack duration

In Layer 7 attacks, the attack duration was similar this quarter when compared to Q1, with an almost balanced split between attacks lasting under 15 mins, up to one hour, and one hour or more.

Attack Duration Q1

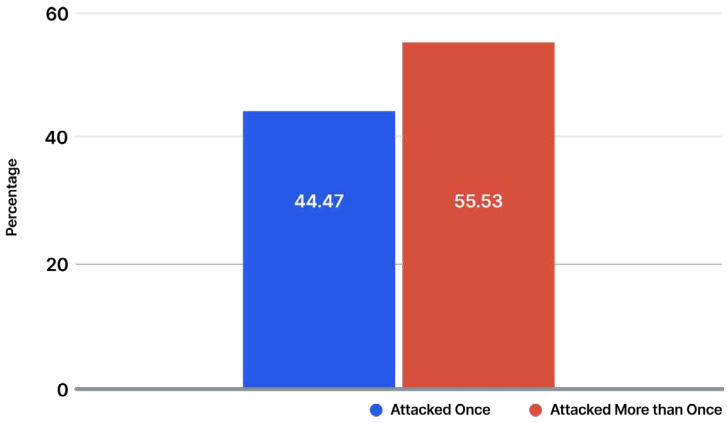


Attack Duration Q2



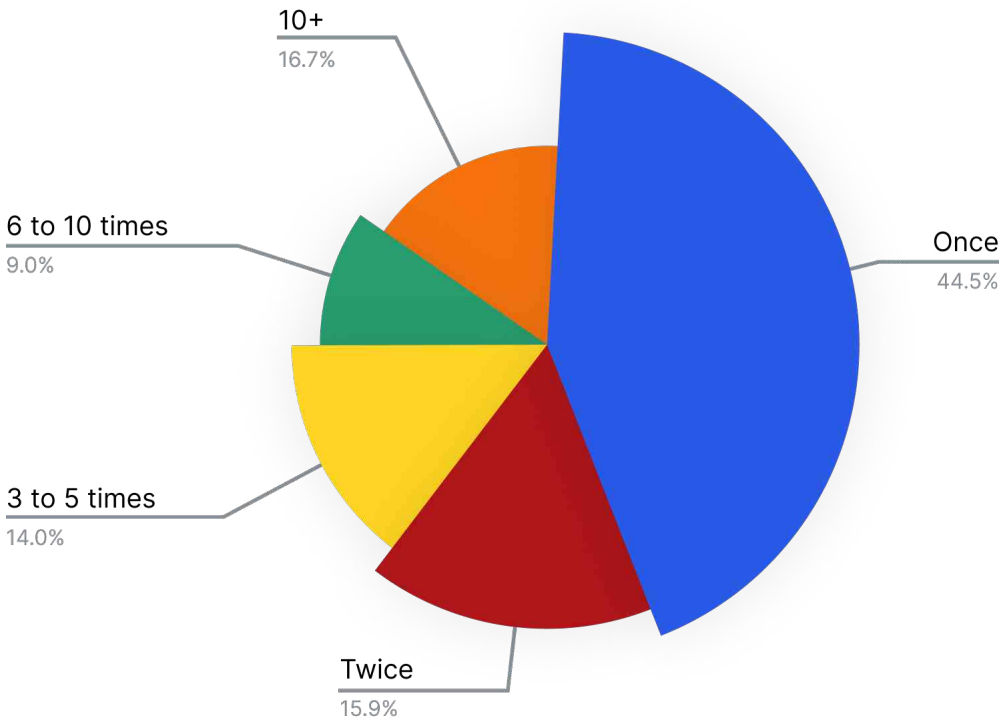
55% of websites hit by a Layer 7 DDoS were attacked again

More than half of the total number of websites attacked in the second quarter of this year were targeted by a further attack, up slightly (around 5%) from Q1. This would suggest that once targeted by an attack for the first time, websites can expect to undergo repeat attacks.



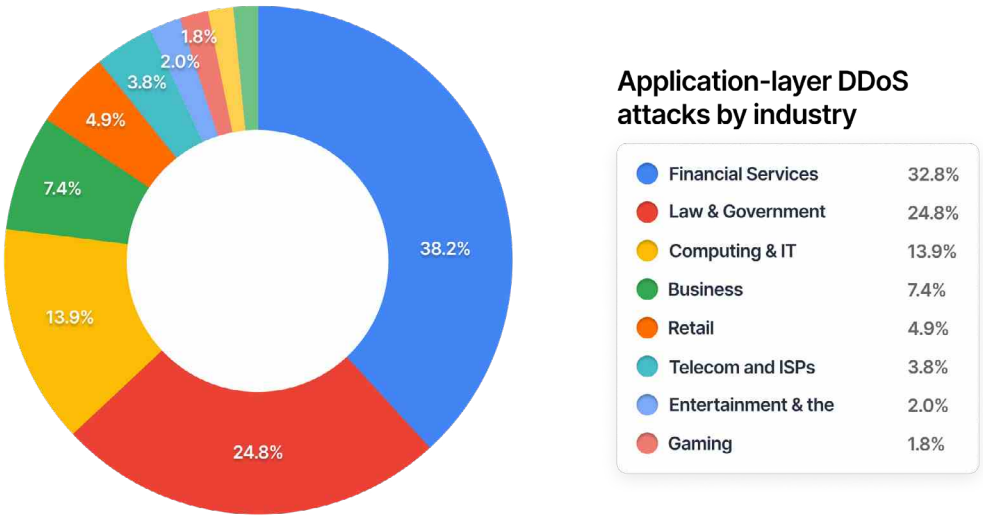
A detailed breakdown of accounts attacked once or more in Q2

No of times customers targeted by Layer 7 attacks



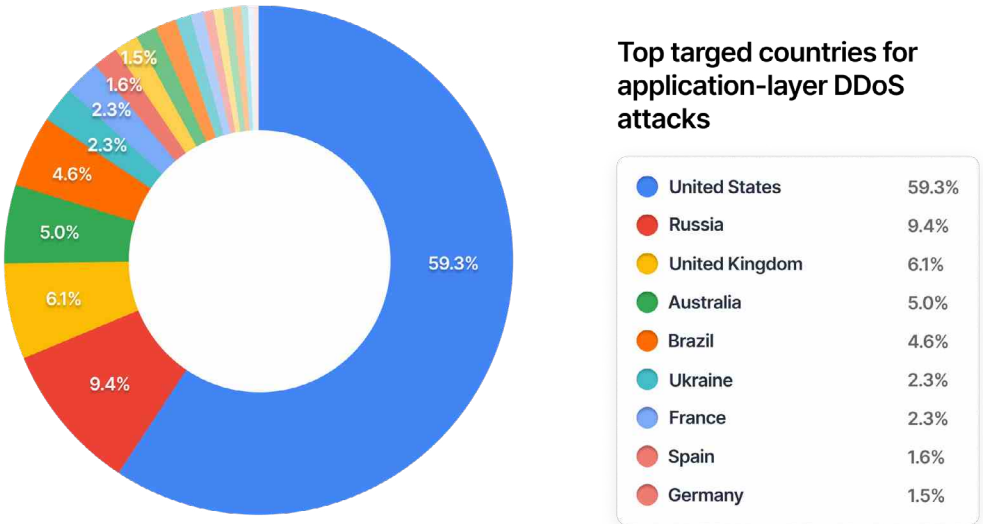
Application-layer DDoS attacks by industry

Financial services, Law and Government, Computing and IT accounted for over 75% of the most targeted industries in Q2 for application-layer DDoS attacks.



Application-layer DDoS attacks - top targeted countries

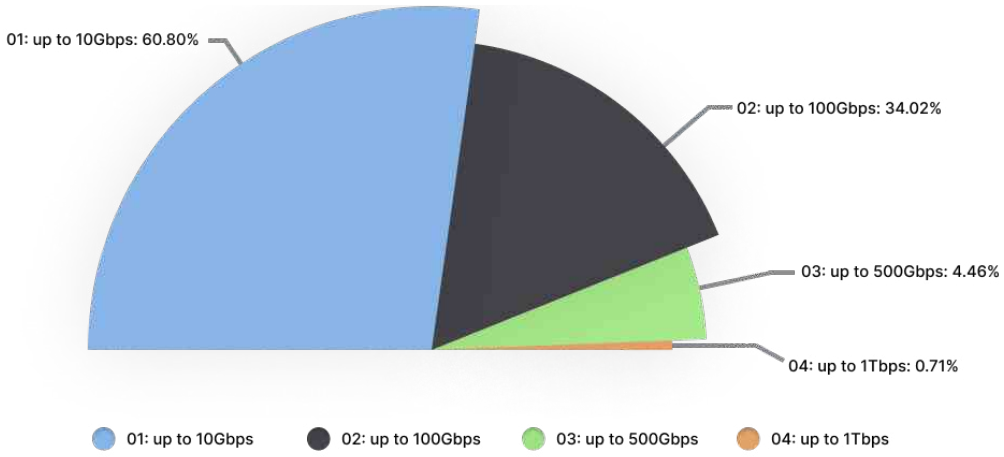
The top targeted countries in Q2 for application-layer DDoS attacks were the US, Russia, and the United Kingdom.



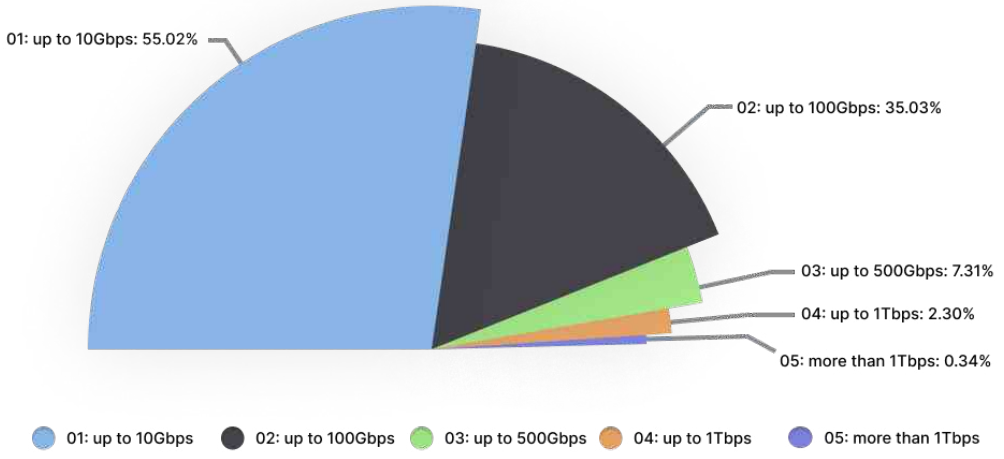
Network-Layer DDoS Attacks

While the number of network-layer DDoS attacks in Q2 decreased compared to Q1, the number of attacks larger than 100 Gbps doubled in Q2 over Q1, and attacks larger than 500 Gbps/0.5 Tbps increased by 287%, suggesting that attackers are focusing on bigger and stronger attacks than before.

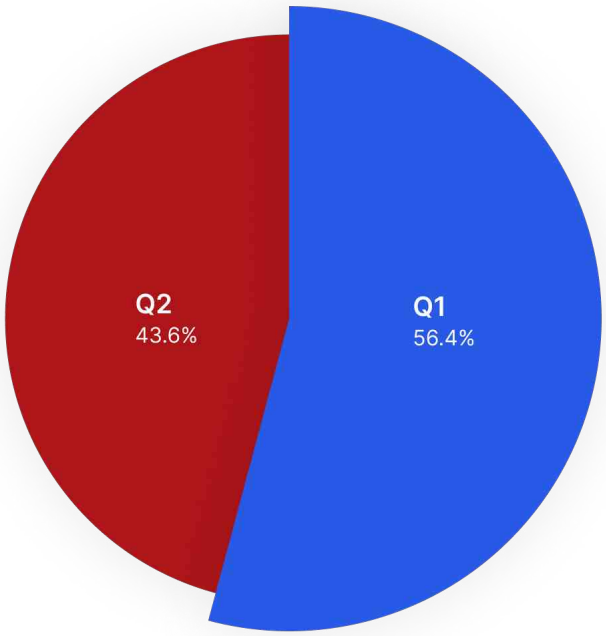
Q1: Attacks by max bw - higher than 1 Gbps



Q2: Higher volume increase in Q2



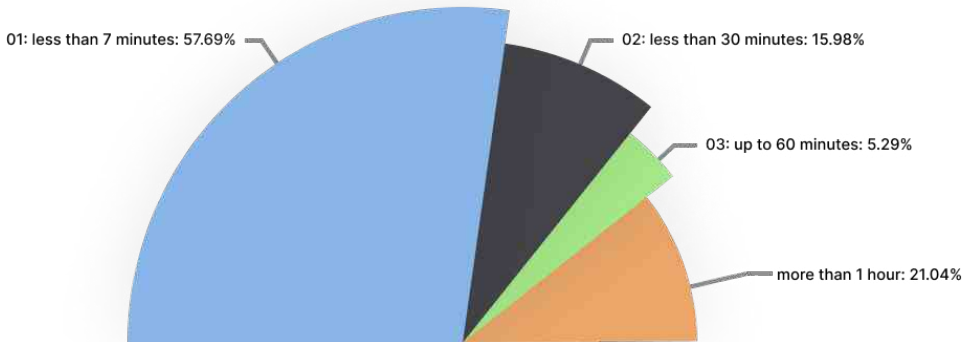
No of network-layer DDoS attacks Q1 vs Q2



Attack duration

In Q2, 21% of attacks lasted over one hour, much as in Q1, where attacks of this duration accounted for 20.6% of all layers 3 and 4 DDoS attacks. Around 60% of network-layer attacks in Q2 were less than seven minutes in duration, which is very similar to Q1 with almost 62%.

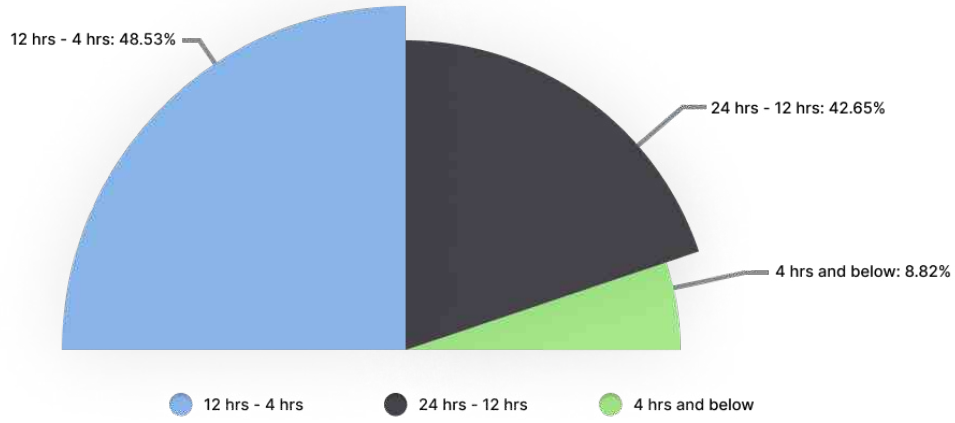
This is further evidence of the importance of Time to Mitigation (TTM) when it comes to choosing the right DDoS mitigation vendor. Imperva guarantees a 3-second SLA for all types of DDoS attacks, no matter the size or the duration, with most attacks mitigated in under one second.



Overall attack duration Q2

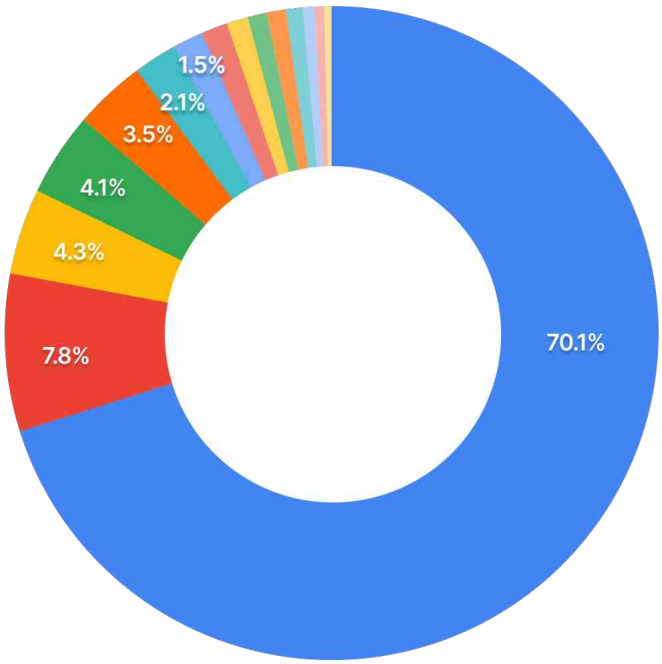
Repeat attacks

In Q2, 80% of customers with network-layer DDoS experienced another attack, which in 91% of cases was carried out within the next 24 hours.



Network-layer DDoS attacks by country

The top-targeted countries for network-layer DDoS attacks in Q2 were the United States, Taiwan, and Poland.

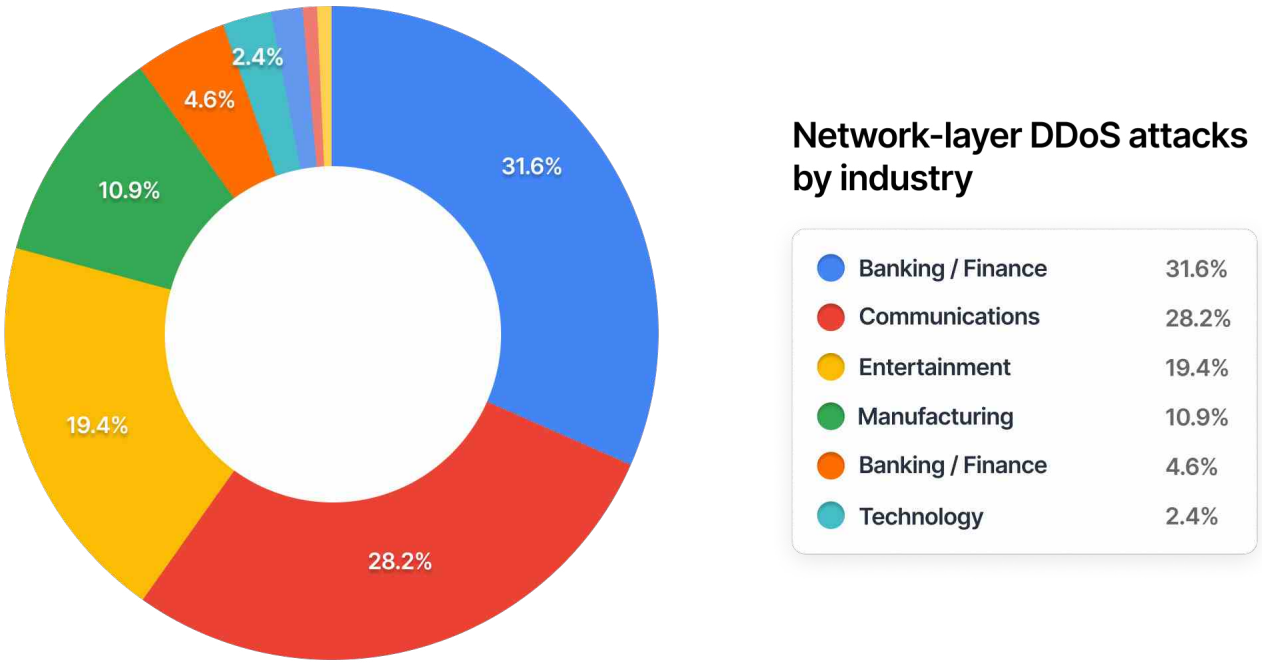


Top targeted countries for network-layer DDoS attacks

United States	70.1%
Taiwan	7.8%
Poland	4.3%
Canada	4.1%
Australia	3.5%
Philippines	2.1%
Spain	1.5%

Network-layer DDoS attacks by industry

The top industries to come under attack by network-layer DDoS attacks in Q2 were Financial Services, Communications, and Entertainment, accounting for almost 75% of all attacks.



Industry Spotlight: Gambling

DDoS attackers double down on gambling sites in Q2

The gambling industry continues to be a lucrative target for cybercriminals, with the increasing popularity and availability of web applications for mobile devices as well as emerging technologies such as VR headsets, IoT, and blockchain. The global online gambling market is expected to grow from $73.42 billion in 2021 to $81.08 billion in 2022[3].

DDoS attacks can disrupt service or shut down whole online casinos and other betting platforms, leading to a loss of revenue and consumer trust. Many DDoS attacks in the gambling market are meant to drive customers away from their preferred platforms to competitor sites to place their bets, which, during real-time sporting and poker events, can hit businesses especially hard.

Odds are, if you're in the gambling industry, your online business will experience DDoS attacks. Asia-Pacific was the largest region in this market in 2021. In 2022, 5 out of 10 accounts that were attacked were from Asia. Around the globe, Imperva has observed a heightened frequency and number of DDoS attacks in the gambling industry in 2022 – 40% of gambling sites were attacked in the last 12 months, and 80% were attacked more than once. In Q2, 25% of gambling sites were attacked in the last month, and 10% of gambling sites were attacked in the final week of the quarter.

To put this in perspective, if an online gambling company generates $1 billion in revenue per year, a sustained DDoS attack would put them at risk of losing approximately $115K per hour. With 80% of gambling sites attacked more than once that is a substantial amount of lost revenue, making DDoS attacks a significant challenge for this industry.

3_https://www.businesswire.com/news/home/20220228005540/en/Global-Online-Gambling-Industry-Analytics-and-Projections-2022-2026---ResearchAndMarkets.com

DDoS in the news

DDoS attacks remain the weapon of choice in cyber-warfare

In DDoS news around the globe, DDoS attacks stemming from the Russia-Ukraine situation still dominate the news as cyber-attacks threaten to escalate military conflict and pro-Russian hacktivists attack a range of European targets. Also in the news, DDoS for hire services remain popular despite a recent crack-down on suppliers.

Cyberattacks could escalate a military conflict

After reports that Russia's Ministry of Construction, Housing, and Utilities website was hacked with a pro-Ukraine message, the Russian government reportedly warned the U.S. and its allies that any cyber attacks on its infrastructure could escalate tensions and result in a "direct military clash" should they continue[4].

Ukrainians DDoS Russian Vodka Supply Chains (May 2022)

Ukrainian hacktivists disrupted vodka shipments in Russia after committing DDoS attacks on a shipment registration portal. While this attack only caused a temporary delay, one firm had to stop alcohol shipments for an entire day[5].

Crack-down on DDoS-for-hire services

DDoS for Hire boss sentenced to prison

In June of Q2, a "Downthem" DDoS-for-hire boss, whose services allowed customers to launch over 200,000 attacks[6], was sentenced to two years in prison. Governments are cracking down on these activities, however, DDoS-for-hire services still contribute to a majority of daily DDoS attacks launched all over the world. Cybercriminals continue to weigh reward over risk by using DDoS and botnets to ransom targets and disrupt websites for maximum profits.

FBI seizes domains used to sell DDoS services

The FBI disrupted malicious DDoS operations this quarter by seizing three domains used by cybercriminals to not only sell sensitive data but also provide DDoS-for-hire services to other criminals[7].

4_https://www.infosecurity-magazine.com/news/russia-cyberattacks-escalate
5_https://www.infosecurity-magazine.com/news/ukrainians-ddos-russian-vodka
6_https://krebsonsecurity.com/2022/06/downthem-ddos-for-hire-boss-gets-2-years-in-prison
7_https://www.bleepingcomputer.com/news/security/fbi-seizes-domains-used-to-sell-stolen-data-ddos-services/

About Imperva

Imperva is the comprehensive digital security leader on a mission to help organizations protect their data and all paths to it. Only Imperva protects all digital experiences, from business logic to APIs, microservices, and the data layer, and from vulnerable, legacy environments to cloud-first organizations. Customers around the world trust Imperva to protect their applications, data, and websites from cyber attacks..

Have you experienced an attack? Contact Imperva

Definitions

Application-layer DDoS Attack

A layer 7 DDoS attack or Application Layer attack sends traffic to use up resources and prevent a website from delivering content uninterrupted. Composed of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web or application server, and the magnitude is measured in Requests per second (Rps).

Network-layer DDoS Attack

Network-layer DDoS attacks or layer 3 and Layer 4 DDoS attacks are volumetric DDoS attacks on a network infrastructure Layer 3 (network layer) and 4 (transport layer). Layer 3 and 4 DDoS attacks are usually measured in Bits per second (Bps) and Packets per second (Pps).

Transport Layer

The transport layer, or layer 4, is so-named as it is the fourth layer in the OSI model and manages the delivery and error checking of data packets and the transfer of data between systems and hosts. This layer transmits data using transmission protocols such as UDP and TCP.

HTTP Pipelining DDoS Attack

HTTP Pipelining allows clients to send requests to web servers in batches without waiting for individual responses. Attackers are misusing this feature to launch DDoS attacks achieving high levels of Rps traffic.

HTTP2 Multiplexing DDoS Attack

HTTP2 Multiplexing was designed to use fewer resources and support more users at the same time by way of a single shared connection between the client and the web server instead of multiple connections. It can also be misused to launch sophisticated DDoS attacks using multiple high workload requests in a single TCP connection.

Further definitions of DDoS attack types can be found here.