imperva

Report

The Imperva Global DDoS Threat Landscape Report 2023

Table of Contents

01 About the report **03**

02 Executive Summary **03**

03 DDoS Trends in 2022 . . . . . **04**

- Cyber Warfare and State-Sponsored Hacktivism 04
- DDoS Attacks as a smokescreen 05
- Call for additional protection mechanisms 06
- Why APIs are a Target for DDoS Attacks 06
- Ransom DDoS for financial gain 06
- DDoS attacks for reconnaissance 07

04 Application Layer DDoS Attacks **08**

- Year over Year growth 08
- Largest Application Layer DDoS attack 08
- Application Layer DDoS attacks increasing year on year 09
- Application Layer DDoS attacks growth by industry 09
- Application Layer DDoS Repeat attacks 10
- Application Layer DDoS Attack Duration 10

05 Network Layer DDoS Attacks **11**

- Largest Network Layer DDoS attacks 11
- Single vector attacks up in 2022 11
- New attack vectors 12
- Network Layer DDoS most common attack vectors 12
- Network Layer DDoS most targeted industries 12
- Network Layer DDoS attack duration 13

06 Recommendations for the year ahead **13**

07 About Imperva **15**

About the report

The 2023 Imperva Global DDoS Threat Landscape Report reviews Distributed Denial of Service (DDoS) attack activity during 2022, provides insights into the year's most noteworthy DDoS events and offers recommendations for the year ahead.

The report leverages intelligence provided by Imperva Threat Research based on data from application and network DDoS attacks we have mitigated. It also provides additional observations based on general DDoS activity throughout the year.

REPORT HIGHLIGHTS

Imperva mitigated its largest Layer 7 DDoS attack measuring 3.9 Million Rps

Layer 7 DDoS attacks increased by 82%

46% of websites came under attack more than once

DDoS attacks on financial services increased by 121%

Executive Summary

DDoS attacks continued to disrupt and destabilize organizations, industries and nation-states in 2022.

Application layer DDoS attacks increased by **82%** compared to 2021 with attacks on the financial services sector growing by **121%** year on year.

The largest Application layer DDoS attack mitigated by Imperva in 2022 was a ransom DDOS attack measuring 3.9 million requests per second (Rps).

Repeat attacks continued to be a DDoS trend in 2022 as around **46%** of websites targeted by a DDoS attack were attacked more than once.

The largest Layer 3 and 4 DDoS attack occurred in July and peaked at 1373 gigabits per second (Gbps). Layer 3 and 4 attacks rose dramatically in August 2022 in comparison to any other month of the year.

DDoS Trends in 2022

Cyber Warfare and State-Sponsored Hacktivism

During the first half of 2022, the DDoS threat landscape was dominated by geopolitical events and cyber warfare centered around political unrest between Russia and Ukraine. As tensions escalated, DDoS attacks targeting websites in both countries grew in number and force, respectively, in the first quarter. What's more, many other nations and organizations, perceived to be taking a stance in support of either Ukraine or Russia, also came under DDoS attack by Advanced Persistent Threat Groups (APTs). Some of the countries targeted included Norway, Italy, and Lithuania.

Emergence of Advanced Persistent Threat groups

Ideologically-motivated APTs such as pro-Russian APT, 'KillNet', and pro-Ukrainian APT, 'IT Army of Ukraine', not only targeted their opposing nation with DDoS attacks, but also any countries and organizations seen to be supporting those nations. 'Killnet' started by offering DDoS attacks for hire, but eventually conducted and took responsibility for DDoS attacks on Ukraine and its supporting countries. By April 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) listed 'Killnet' as one of several pro-Russia cybercrime groups which could pose a threat to critical infrastructure organizations. Other APT groups on CISA's list at the time included:

- The CoomingProject
- MUMMY SPIDER
- SALTY SPIDER
- SCULLY SPIDER
- SMOKEY SPIDER
- WIZARD SPIDER
- The Xaknet Team

Conflict-motivated DDoS were not limited to the first half of the year. As late as December 2022, Russia's second-largest financial institution was targeted by a massive DDoS attack. According to an article by Bleeping Computer, VTB Bank said it was facing the worst cyberattack in its history after its website and mobile apps were taken offline due to a DDoS attack.

How Media Events Spark DDoS Attacks

In other parts of the world, DDoS attacks also played a part in state-sponsored hacktivism. Media coverage of the controversial visit by the former U.S. House Speaker Nancy Pelosi to Taiwan in August 2022 sparked a spate of DDoS attacks. This was the first visit to the country by a high-ranking U.S. official in 25 years and it resulted in various scenes of internet chaos including DDoS attacks targeting Taiwanese infrastructure. In the days leading up to the visit, several Taiwanese government websites came under attack with the website of Taiwanese President Tsai Ing-wen reported to have been hit by a DDoS attack that caused traffic levels to the site to surge to 200 times their normal rate. Other Taiwanese websites found to be inaccessible around the same time were linked to the National Defense Ministry, the Foreign Affairs Ministry, and the website of the country's largest airport, Taiwan Taoyuan International.

The events in Taiwan are further examples of how today, geopolitical relations and tensions are almost always accompanied by an increase in targeted and strategic cyber attacks. DDoS attacks are often the 'weapon of choice' by politically motivated

cyber attackers because of the levels of damage and disruption they are capable of causing to critical infrastructure such as government websites and airports.

No one is safe from DDoS

Even the Pope's website is not safe from DDoS attacks. In December 2022, it was reported that a DDoS strike on the Vatican website took it offline for several days, possibly the work of Russian activists. According to a blog by Tech Monitor, "The cyberattack comes days after the Pope was criticized by the Russian government for comments he made about its soldiers fighting in the war in Ukraine".

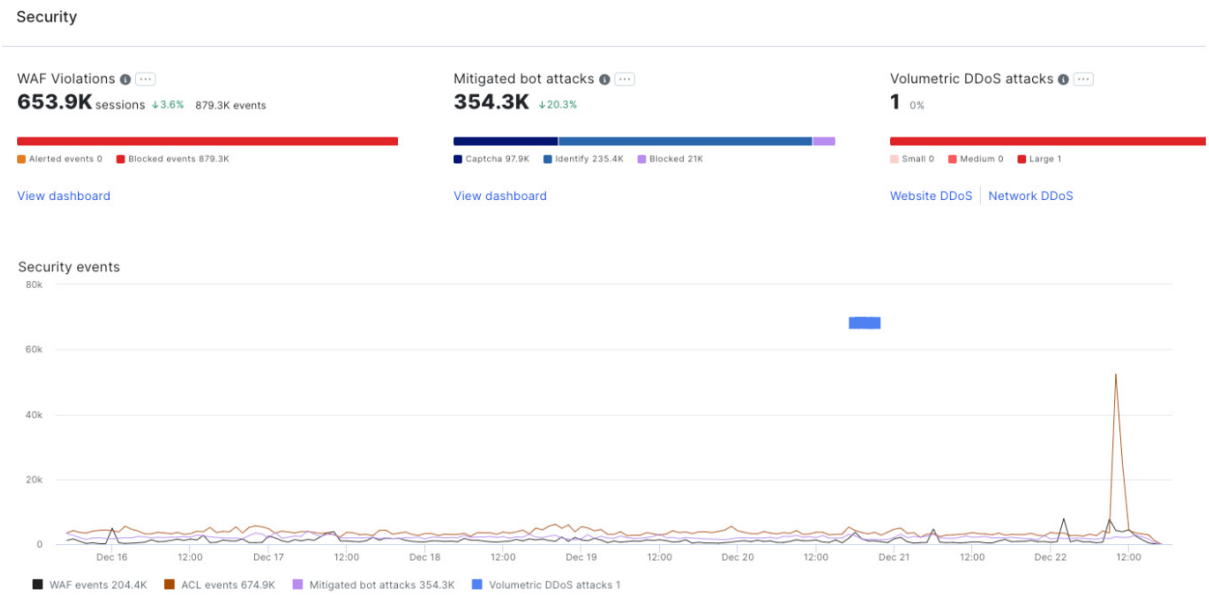
Similar examples of state-sponsored hacktivism were also observed in Israel and in Asia around the same time as political visits and other politically-motivated events were taking place.

DDoS Attacks as a smokescreen

DDoS attacks are often leveraged by cybercriminals as a distraction tactic to launch a further, often more aggressive, attack on a target's infrastructure. In 2022 our Threat Research team monitored several instances where DDoS attacks appeared to be used as a precursor to more complex malicious activity. While it is difficult to link or identify the motivation behind such attacks, there appears to be a continuing trend for cybercriminals leveraging DDoS attacks as a smokescreen to distract security teams. This makes way for further application attacks such as Account Takeover attacks (ATO) or attacks on API endpoints to infiltrate sensitive data.

The example below shows how a volumetric DDoS attack mitigated by Imperva was followed by a series of further attacks including Account Takeover (ATO) and Bot attacks.

The end goal for this type of attack is typically financial reward whereas a DDoS attack's objective is to cause disruption and take a site offline. The profit-making aspect to these attacks makes them more sinister than a DDoS attack and potentially more costly to recover from.



In our blog, 'Lift the DDoS Smokescreen: Investigate Underlying Attacks', we describe how, as attack tactics continued to evolve, large service disruptions often came in parallel with other attack vectors, where, whether intentional or not, DDoS was used as a smokescreen to pivot the defending team's attention away from a more sophisticated and precise simultaneous offense, such as ATO (Account Takeover) or phishing. In 2022, this was a trend we continued to see with cybercriminals launching DDoS attacks as the forerunner to further different attack types in what could be described as an integrated attack strategy.

Call for additional protection mechanisms

The use of DDoS as a smokescreen for further cyber attacks is not going unnoticed. There is a recognition among Imperva customers that a DDoS attack could potentially leave their infrastructure vulnerable to further attacks. Data gathered by Imperva shows that customers are now seeking additional protection mechanisms such as advanced geo-blocking or a Network Access Control List (ACL), to minimize the attack surface from additional (non-DDoS) threats following on from a DDoS attack.

Why APIs are a Target for DDoS Attacks

A shift to more modern applications has meant an explosion in the adoption of API endpoints which, as they become more intrinsic to a company's infrastructure, present new opportunities for cybercriminals to cause disruption.

Around 40% of all web traffic to the Imperva Cloud WAF is API-related and, according to our latest State of Security Within eCommerce in 2022 Report, which states that API traffic now accounts for 41.6% of all traffic to online retailers.

DDoS API attacks target both the server that the API is running on and the API endpoints with the objective of overwhelming the API and impacting performance. A sophisticated DDoS attack will leverage botnets to imitate legitimate traffic and can cause a significant impact on the API endpoints and server.

Hackers like to seek out their target's weak points which is why API endpoints and servers without the right security measures in place are more at risk. Left unprotected, API servers are more vulnerable to DDoS attacks where the attackers use well-crafted API calls. Unable to differentiate between invalid and legitimate requests, significant server resources are wasted parsing and validating invalid API calls before they can be filtered out.

Denial of Wallet DDoS Attacks on Shadow APIs

A Denial of Wallet attack is a risk for Web applications and APIs hosted in the cloud. Similar to a DDoS attack, its goal is to bankrupt its cloud-based target by sending traffic that will result in extortionate charges by the cloud provider. A DDoS attack will try to take your Application or API offline, but due to the nature of the public cloud, serverless architecture resources continue to spin up to try to cope with the load. This is a particular problem when it comes to Shadow APIs as enterprises struggle to track and keep tabs on this type of serverless API and Denial of Wallet attacks targeting this type of serverless application can result in rapidly ballooning costs.

Ransom DDoS for financial gain

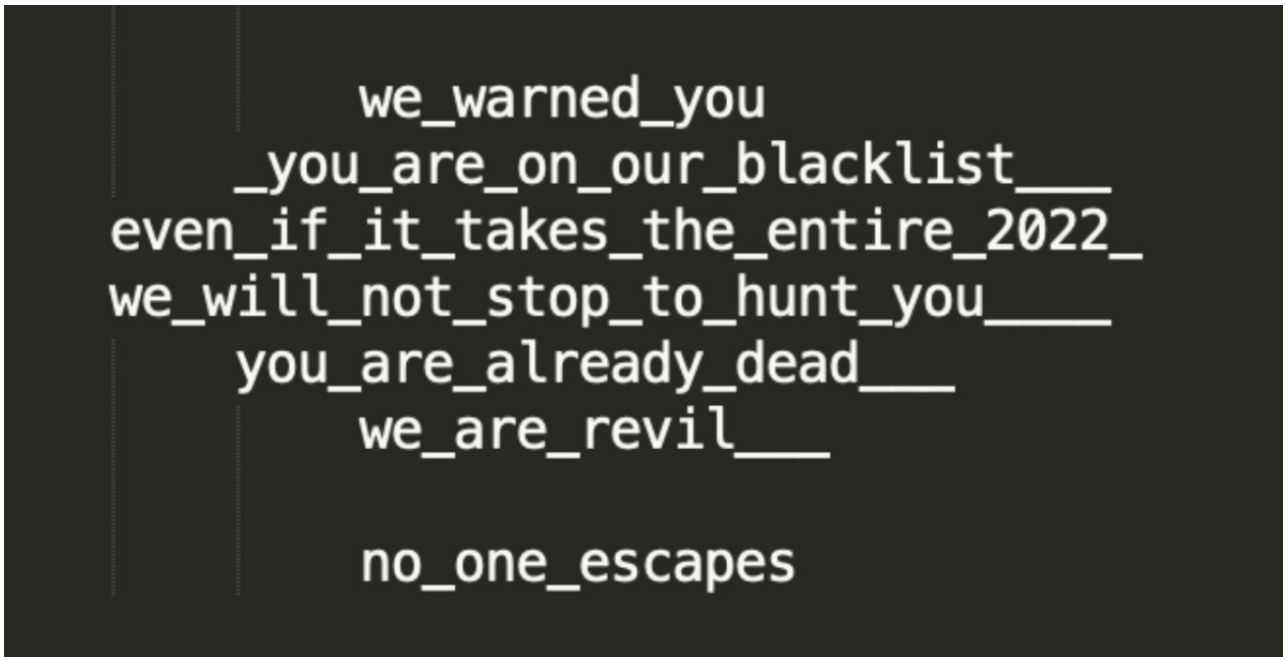
Ransom DDoS attacks typically consist of a demand for payment followed by a small sample DDoS attack to show what the attackers are capable of. If the ransom demands, often requested in bitcoin, are not met, a more forceful DDoS attack or another type of attack often follows. In February 2022, Imperva mitigated a large Layer 7 DDoS attack which took place over several days with similar patterns observed across two attacks including requests sent using real web browsers originating from specific

locations like China, Russia, and Ukraine. These web browsers were accessing the root (/) of the domain. The second pattern observed was the encoding of a ransom note within the URL. This is just one example of the creative techniques applied by attackers in 2022.

DDoS attacks for reconnaissance

Attackers often use DDoS attacks as a way of scoping out their target. To measure the strength of their defenses and to assess how much additional force they need to apply. In this instance the initial DDoS attack was likely a reconnaissance attack, leading up to a larger effort a few days later.

In another ransom DDoS attack in the same month, also claimed by a group naming themselves the well-known Ransomware as a service (RaaS) operator REvil', the targeted company was hit by several DDoS attacks; the largest of which lasted less than one minute and measured up to 2.5 Mrps, setting a new mitigation record for Imperva at the time. Multiple sites from the same company came under attack with one site sustaining an attack lasting around 10 minutes. The attackers applied sophisticated tactics to avert mitigation with the ransom messages and attack vectors changing constantly.



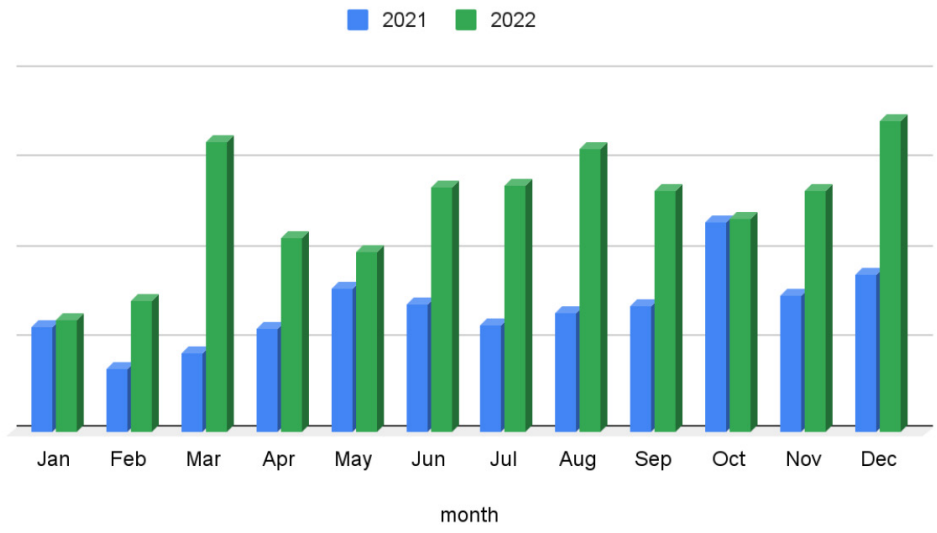
Example of a ransom threat note embedded within a URL request in this case from a group claiming to be Advanced Persistent Threat group 'Revil'

In this case, the attack lasted several days with the attackers applying various scare tactics with the objective being to achieve as much financial gain as possible. Fortunately for the customer, Imperva successfully mitigated all of the attacks demonstrating the importance of having a DDoS solution in place with a fast mitigation SLA.

Application Layer DDoS Attacks

Year over Year growth

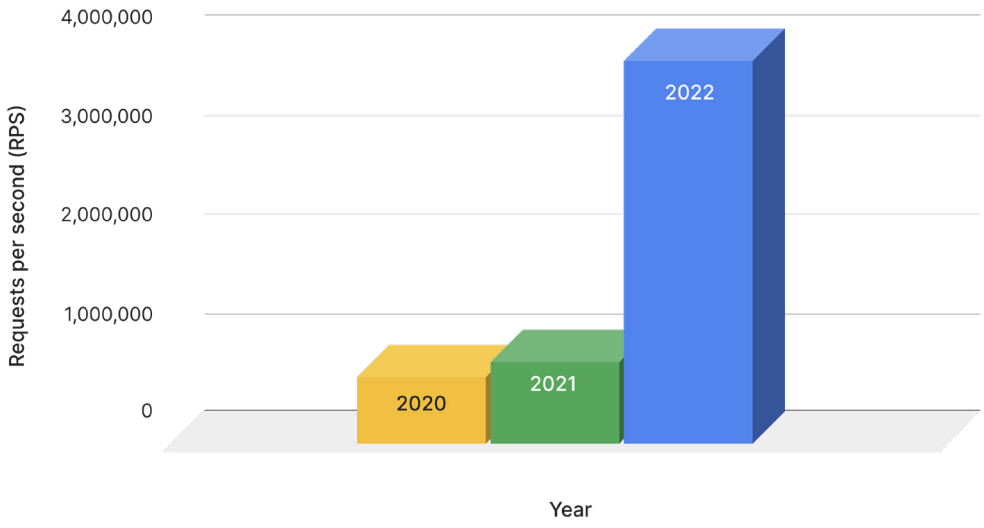
Application Layer (L7) DDoS attacks increased by a staggering **82%** YoY in 2022 vs 2021. The number of incidents surged in Q1 when geopolitical events in Europe were the driving force behind increased DDoS activity against the countries involved and those seen to be supporting them. In March 2022 Imperva mitigated **more than 3.5X** the number of Application DDoS attacks than during the same month the previous year.



Increase in Application Layer DDoS attacks 2022 vs 2021

Largest Application Layer DDoS attack

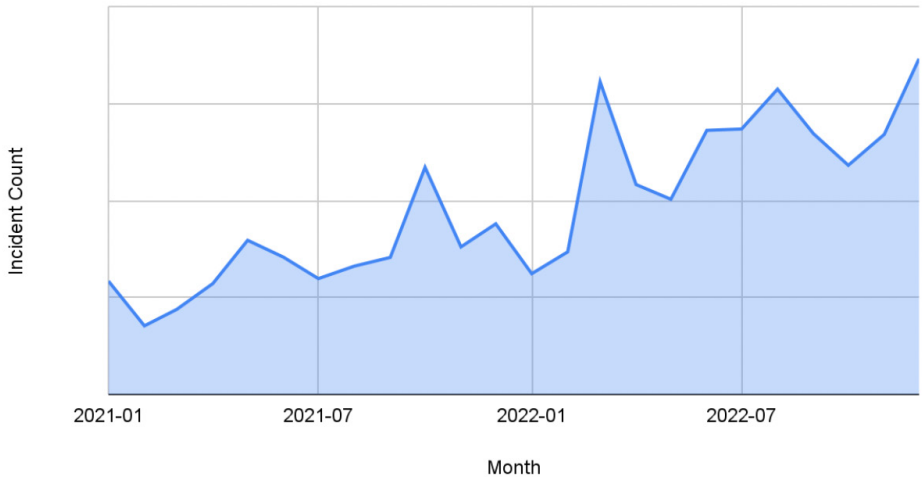
Imperva mitigated its largest application layer DDoS attack in June measuring 3.9Mrps. Application layer DDoS attacks continue to grow in force (RPS) year over year.



Application Layer DDoS attacks growing year by year

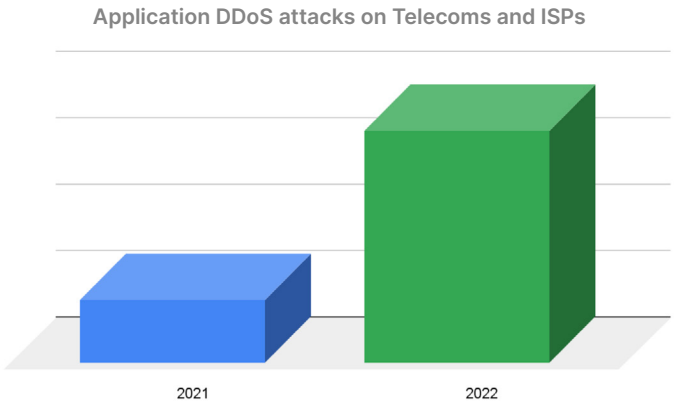
Application Layer DDoS attacks increasing year on year

The number of application layer DDoS attacks has been on an upward trajectory year on year as the chart below shows, a clear indication that DDoS attacks aren't going away anytime soon. DDoS is a valuable tool, and attackers know it's a good method to use for extortion or hacktivism. The bar for accessing DDoS as an attack method for threat actors is being lowered each year in terms of availability and cost. There are many reasons for this trend not least the expansion of connected IoT devices is also a contributing factor in the growth of DDoS attacks

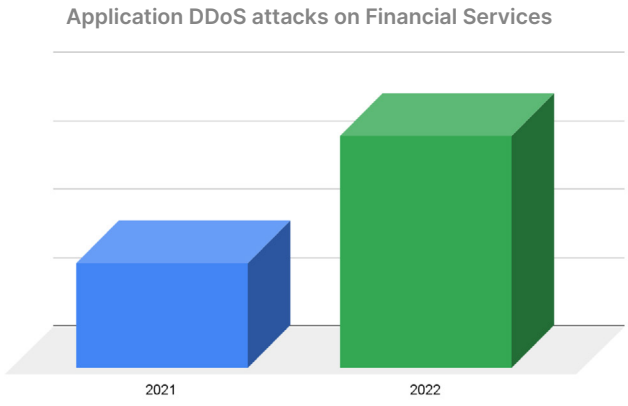


Application Layer DDoS attacks trending upwards YoY

Application Layer DDoS attacks growth by industry



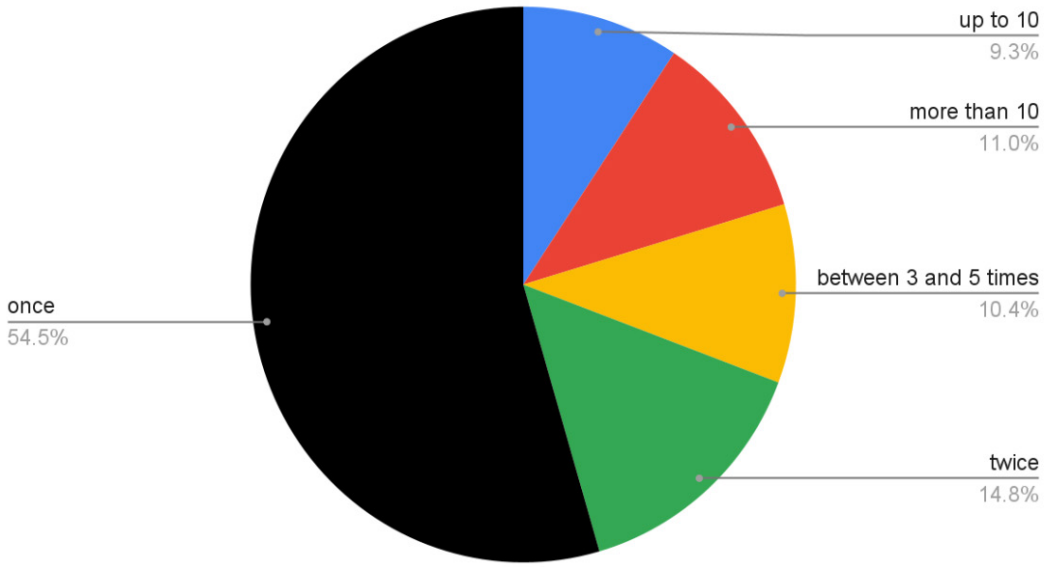
Application Layer DDoS attacks on the Telecoms and Internet Services Provider (ISP) sector increased by 250% in 2022 vs 2021.



Application Layer DDoS attacks on Financial Services more than doubled in 2022 compared to the previous year's increase by 121%.

Application Layer DDoS Repeat attacks

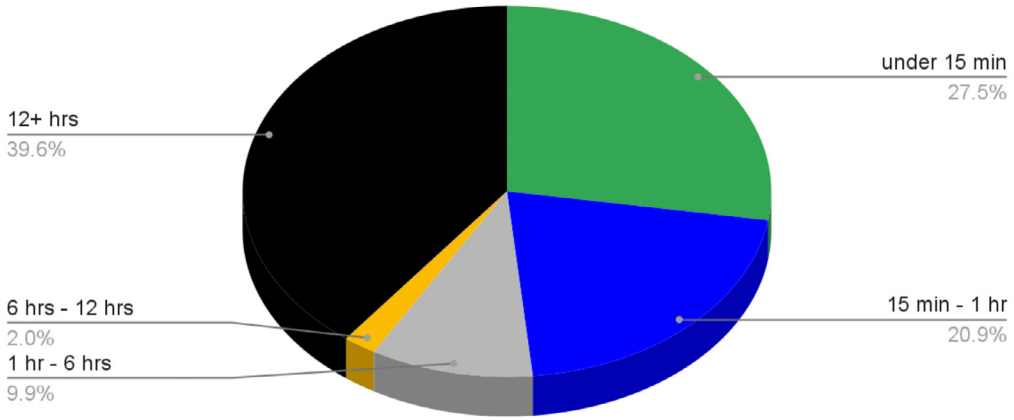
46% of all sites targeted by an Application Layer DDoS attack in 2022 were targeted more than once during the same year. This would indicate a growing trend for websites undergoing repeat attacks and possibly even extortion attempts once targeted for the first time.



Sites targeted by a DDoS attack multiple times

Application Layer DDoS Attack Duration

Our research shows that Layer 7 DDoS attack duration is becoming longer in duration with almost 40% of all Layer 7 DDoS attacks lasting more than 12 hours, an increase of 33% of attacks in 2021.



Application Layer DDoS attack duration 2022

Network Layer DDoS Attacks

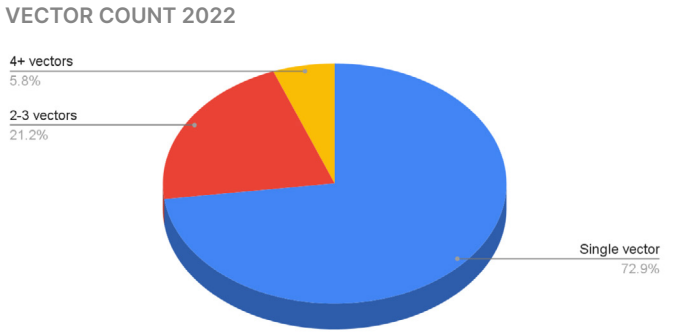
Largest Network Layer DDoS attacks

The largest volumetric DDoS attack Imperva mitigated in 2022 was in July with a peak of 1373 gigabits per second (Gbps). During the attack the most common vector used was sum_dns_response.

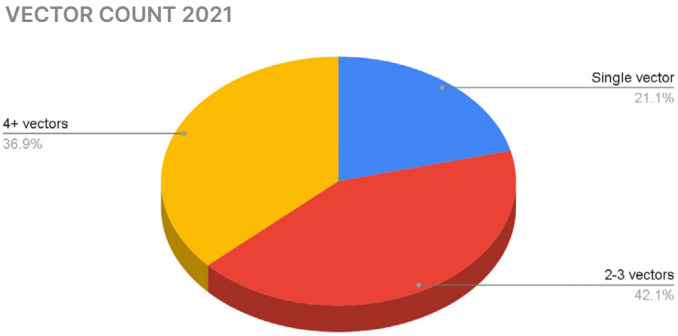
The largest protocol attack mitigated peaked at 591 million packets per second (Pps). This attack was mitigated in October and the most common vector used during the attack was Sum NTP and SUM SSDP.

Single vector attacks up in 2022

In 2022, almost 73% of all layer 3 and 4 DDoS attacks consisted of a single vector which is in sharp contrast to 2021 when only 21% of attacks were single-vector. This might indicate that DDoS attackers are leveraging single vector attacks as part of a wider attack strategy possibly as a distraction tactic.



Single-vector DDoS attacks should not be underestimated as persistent, short single-vector attacks on a network where the legacy DDoS solution is configured to ignore this level of activity could result in network performance being impacted before the DDoS mitigation has had a chance to recognize the issue and kick into action.



New attack vectors

In 2022, we reported that two new attack vectors had emerged and were observed in DDoS attacks mitigated by Imperva.

TCP Middlebox Attacks

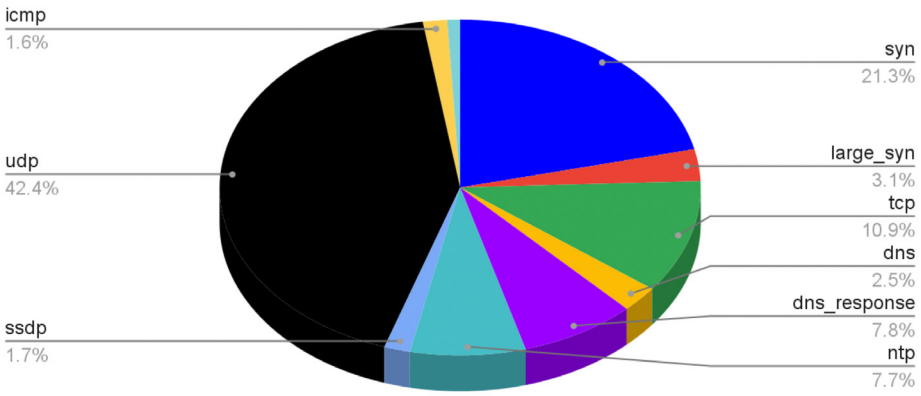
TCP Middlebox Amplification attacks were first revealed in August 2021 in a paper written by academics from the University of Maryland and the University of Colorado. In these attacks, a new amplification technique, TCP Middlebox Reflection, leverages non-compliant TCP middlebox servers to induce them to respond and amplify network traffic against their victims.

UDP TP240

A second new reflection/amplification DDoS vector emerged in early 2022 known as TP240PhoneHome. First observed by researchers in February, attackers used this vector to abuse a large number of TP-240 VoIP-processing systems to launch multiple high-impact attacks.

Network Layer DDoS most common attack vectors

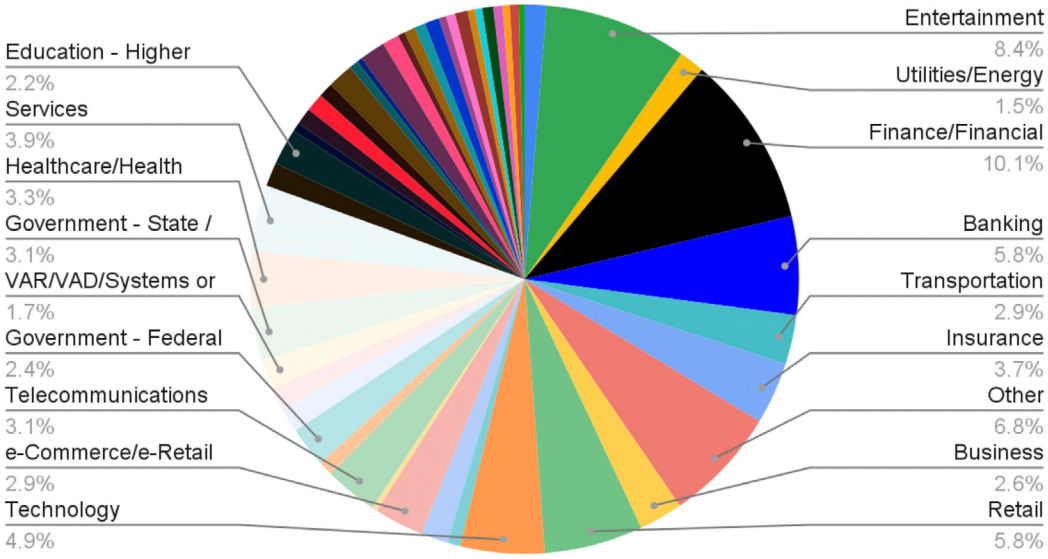
The most commonly observed attack vectors in layer 3 and 4 DDoS attacks in 2022 as mitigated by Imperva were UDP, SYN, and TCP.



Most common attack vectors

Network Layer DDoS most targeted industries

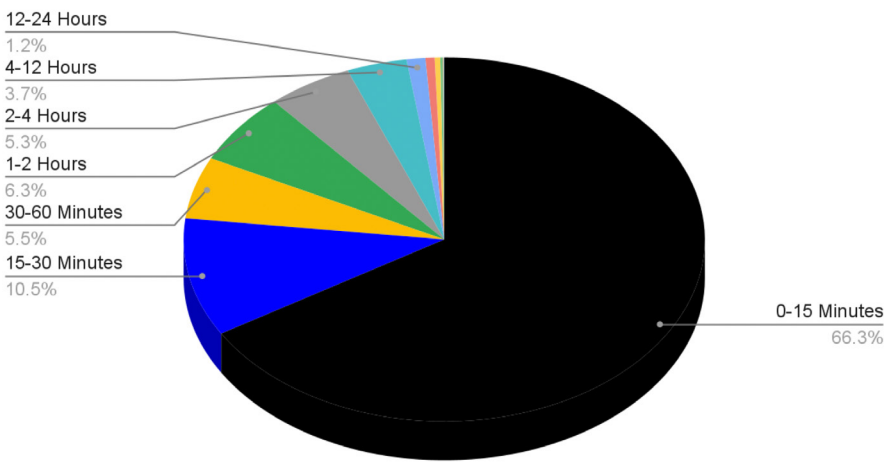
Financial Services and Banking targets accounted for around 16% of all network layer DDoS attacks in 2022 followed by the Entertainment industry at 8.4%.



Network Layer DDoS - Attacked Accounts by Industry

Network Layer DDoS attack duration

66% of all Network Layer DDoS attacks mitigated by Imperva lasted 15 minutes or less in 2022.



Recommendations for the year ahead

The findings in this report demonstrate that DDoS attacks are still a very popular choice for cyber criminals and hacktivists hoping to cause maximum disruption and therefore they represent a genuine threat to organizations.

Our data would also indicate that attackers are leveraging DDoS attacks as a smokescreen for a more advanced attack or series of attacks, not limited to DDoS.

This also works in reverse when a series of application attacks culminate to become a DDoS attack. Our research shows that attackers are using botnets to launch application attacks such as API fuzzing, account creation, brute-force attacks and scraping, which eventually culminates to become a DDoS attack.

APIs are a top target for DDoS attacks and can result in damage to brand reputation if taken offline, or in hefty charges if targeted by a Denial of Wallet attack in the public cloud.

While the report highlights DDoS attacks targeting certain industries such as governments and financial services, many other industries come under attack too. No one is safe from a DDoS attack.

To ensure you are protected we have put together a list of recommendations when choosing a DDoS Protection vendor.

- Opt for 'Always-On' DDoS Protection as it will kick in faster to start mitigating the short single vector attacks that might otherwise, slip under the radar.
- Choose a DDoS solution with a short SLA written into your contract.
- Consider implementing a Contingency DDoS solution to ensure your networks are always protected even in the event of an outage at your primary provider.
- Remember that a DDoS attack might precede or follow a series of other attacks. Take a combined approach to mitigation by choosing a security platform equipped to protect your infrastructure from all the latest threats.

Definitions

Layer 7 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). Application layer attacks are harder to detect as the attacker appears to be sending a normal request like a legitimate website user.

Layer 3 and 4 DDoS Attack

Layer 3 and Layer 4 DDoS attacks or infrastructure layer attacks are types of volumetric DDoS attacks on a network infrastructure Layer 3 (network layer) and 4 (transport layer). DDoS attacks consume high volumes (floods) of data to slow down web performance, deplete bandwidth, and eventually take your services offline completely. Layer 3 and 4 DDoS attacks are usually measured in Bits per second (Bps) and Packets per second (Pps).

Network Layer

The network layer or layer 3 is so-named as it is the third layer in the OSI model and refers to bandwidth capacity. The aim of a DDoS attack on the network layer is to overwhelm bandwidth and prevent the network from routing information to where it needs to go next, which subsequently impacts performance and can bring the network to a complete standstill.

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.

Volume Based Attack

Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

Protocol Attack

Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, and more. Measured in PPS this type of attack consumes actual server resources, or intermediate communication equipment such as firewalls and load balancers.

Ransom DDoS Attack

A ransom DDoS attack is an extortion-based threat, motivated by easy, low-risk financial gain. Attackers send an email demanding payment, often in Bitcoin, to avoid a DDoS attack.

API Fuzzing

API fuzz testing is an automated testing method whereby random, invalid data is input into the API to help discover bugs and potential security issues.

Brute Force Attack

Brute-force attacks or 'hammering' attacks consist of the submission of many passwords or passphrases with the hope of eventually guessing correctly.

Scraping

Web-scraping refers to the automated extraction of data, often publicly available, from a website or websites and putting it into a more usable format for the end user.

Further definitions of DDoS attack types can be found here.

About Imperva

Imperva is the cybersecurity leader whose mission is to help organizations protect their data and all paths to it. Customers around the world trust Imperva to protect their applications, data, and websites from cyber attacks. With an integrated approach combining edge, application security, and data security, Imperva protects companies through all stages of their digital journey. The Imperva Threat Research team and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy, and compliance expertise into our solutions.