imperva

Landscape Report

Imperva DDoS Threat Landscape Report Q1 2022

A quarterly summary of distributed denial of service (DDoS) attack activity as monitored and mitigated by Imperva during the first quarter 2022

Table of Contents

About the Q1 2022 Threat Landscape Report

With world and market events significantly impacting the pace at which the DDoS threat landscape can change, we are increasing the frequency of our reporting from annual to quarterly. This report is the first in the new quarterly cadence.

The purpose of the new quarterly report is to bring you the latest and most up to date observations from Imperva Research Labs on a more regular basis to raise awareness and inform you about DDoS attacks and their potential impact on businesses and global affairs.

The Q1 2022 report is based on analysis of DDoS attacks targeting Imperva customers in the first three months of the year, with data collected from our global network of 50 DDoS-resilient Points of Presence (PoPs) and over 9 TeraBytes Per Second (Tbps) of capacity.

HIGHLIGHTS

We mitigated our biggest attack **measuring 2.5 million rps**

70% increase in the number of Layer 3 and 4 DDoS attacks

50% of all sites hit by a DDoS attack were targeted a second time

73% increase in volume of DDoS attacks on targets in Ukraine

60% of Layer 3 and 4 attacks lasted 7 **minutes or less**

Executive Summary

A turbulent start to the year as cyber warfare and new attack vectors impact DDoS attacks around the world

During the first three months of 2022, major global events impacted the DDoS landscape. Firstly, and most significantly, the current geopolitical environment has caused worldwide caution regarding the heightened possibility of a cyber attack. As a result the U.S. Cybersecurity and Infrastructure Security Agency (CISA), a United States federal agency under the oversight of the Department of Homeland Security, issued guidance for business leaders and those responsible for digital security to prepare for attacks and adapt their digital security posture.

With the onset of the conflict in Ukraine, the month of March had the highest number of attacks in Q1, likely the result of an increase in DDoS attacks in Russia and Ukraine as well as globally, as cyberwarfare escalated. This report captures how in early March DDoS attacks targeting sites in Russia and Ukraine spiked in number and in volume respectively.

Also driving up attack volumes this quarter were new attack vectors TCP Middlebox Amplification and UDP TP240 PhoneHome being used in DDoS attacks on several of our customers. These new vectors saw threat actors exploiting vulnerabilities in network services to amplify the impact of their attacks.

Finally in Q1 we mitigated our largest application DDoS attack to date: in February, a Layer 7 attack on one single site reached 2.5 million requests per second (Mrps). This was one of several attacks on the same company during which multiple sites came under attack.

Layer 7 DDoS Highlights

Attack volumes on Ukrainian sites grew by 73%

An increase of **73%** in Layer 7 DDoS attack volume was reported during the first quarter highlighting how cybercrime is very much a factor of modern-day warfare.

Imperva mitigated its largest Layer 7 attack measuring 2.5 Mrps

In February we mitigated our largest DDoS attack ever measuring over 2.5 million requests per second (Mrps). The attack was a multifaceted ransom DDoS attack against a single site, which was followed by several threats and demands for payment. The attackers used a novel tactic of embedding a ransom note into a url request. In the same DDoS attack, Imperva mitigated over 12 million such embedded requests targeting random URLs on the same site.

18%+ of Layer 7 attacks lasted more than 12 hours

More than **60%** of all Layer 7 attacks mitigated by Imperva in Q1 lasted over 15 minutes, with almost **20%** sustained for more than 12 hours. This type of prolonged attack can cause extensive damage in terms of application accessibility, loss of customers, and recovery costs.

50% of websites hit by a Layer 7 DDoS were attacked again

More than half of the total number of websites attacked in the first quarter of this year were targeted by a further attack. This would suggest that once targeted by an attack for the first time, websites can expect to undergo repeat attacks.

Ransom DDoS Threats continue to disrupt

Ransom Denial of Service threats continue to present a challenge, with threat actors using more innovative tactics to disrupt business and attempt to extort payment. In the 2.5 Mrps attack the threat was embedded into a URL request, making it part of the attack itself and reminding the target to pay the amount demanded in bitcoin.

Layers 3 and 4 DDoS Highlights

4X increase in attacks on websites in Ukraine and Russia

Between January and February 2022, attacks on Russian and Ukrainian websites increased fourfold as Imperva reported an increase of **320%** in attacks month on month.

DDoS attacks increased overall by 70% in March

The number of attacks almost doubled from January to February 2022, with an increase in Layers 3 and 4 attacks of **70%**.

Almost 80% of attacks were single-vector

Only **20%** of Layers 3 and 4 DDoS attacks used more than one vector in Q1, with the remaining attacks all being single-vector. This would appear to buck the trend in recent years for multi-vector attacks, which target different network layers simultaneously, making mitigation more challenging. However, the impact of single-vector DDoS attacks should not be underestimated as **a network is only as safe as the DDoS protection in place**. For example, repeated short single-vector attacks on a network where the legacy DDoS solution is configured to ignore this level of activity could result in slower performance as the network becomes overwhelmed before mitigation has a chance to kick in.

More than 60% of attacks lasted 7 minutes or less

Layer 3 and 4 DDoS attacks were quite short in duration during Q1, with almost **62%** of all attacks lasting seven minutes or less. Shorter attacks are dangerous for a number of reasons and are often used as a distraction tactic as part of a wider, multi-vector attack.

New attack vectors on the rise

Imperva observed a significant number of the new DDoS attack vectors of TCP Middlebox Amplification and UDP TP240 PhoneHome DDoS attacks, with attackers exploiting vulnerabilities in network services to amplify the impact of their attacks.

Layer 7 DDoS attacks

Imperva mitigated its largest attack so far

In February we mitigated our largest DDoS attack to date. The Layer 7 attack—part of a wider ransom DDoS extortion attempt by a group claiming to be well-known hacktivist group 'REvil'[1], who launched several DDoS attacks, the largest of which measured up to 2.5 million requests per second—set a new mitigation record for Imperva. During the attack, multiple sites from the same company were targeted, with one attack being sustained for around 10 minutes. Before the first attack began, the target had received several warning ransom notes with some of the demands embedded into site urls.

```
we_warned_you
_you_are_on_our_blacklist_
even_if_it_takes_the_entire_2022_we_will_not_stop_to_hunt_you_
_you_are_already_dead_
we_are_revil_

no_one_escapes
```

The following day on the same site, Imperva mitigated over 15 million requests, this time with the URL containing a different message but using the same scare tactics warning the CEO that they are going to destroy the company's stock price if they don't pay up.

```
entryURL: "GET www.[redacted].com let_your_ceo_know_that_we_are_not_going_to_destroy_
[redacted]_stock_price_like_we_do_with_bandwidth_better_to_start_paying
_1_bitcoin_per_day_bc1q[redacted]zz_revil_this_is_our_domain_"
```

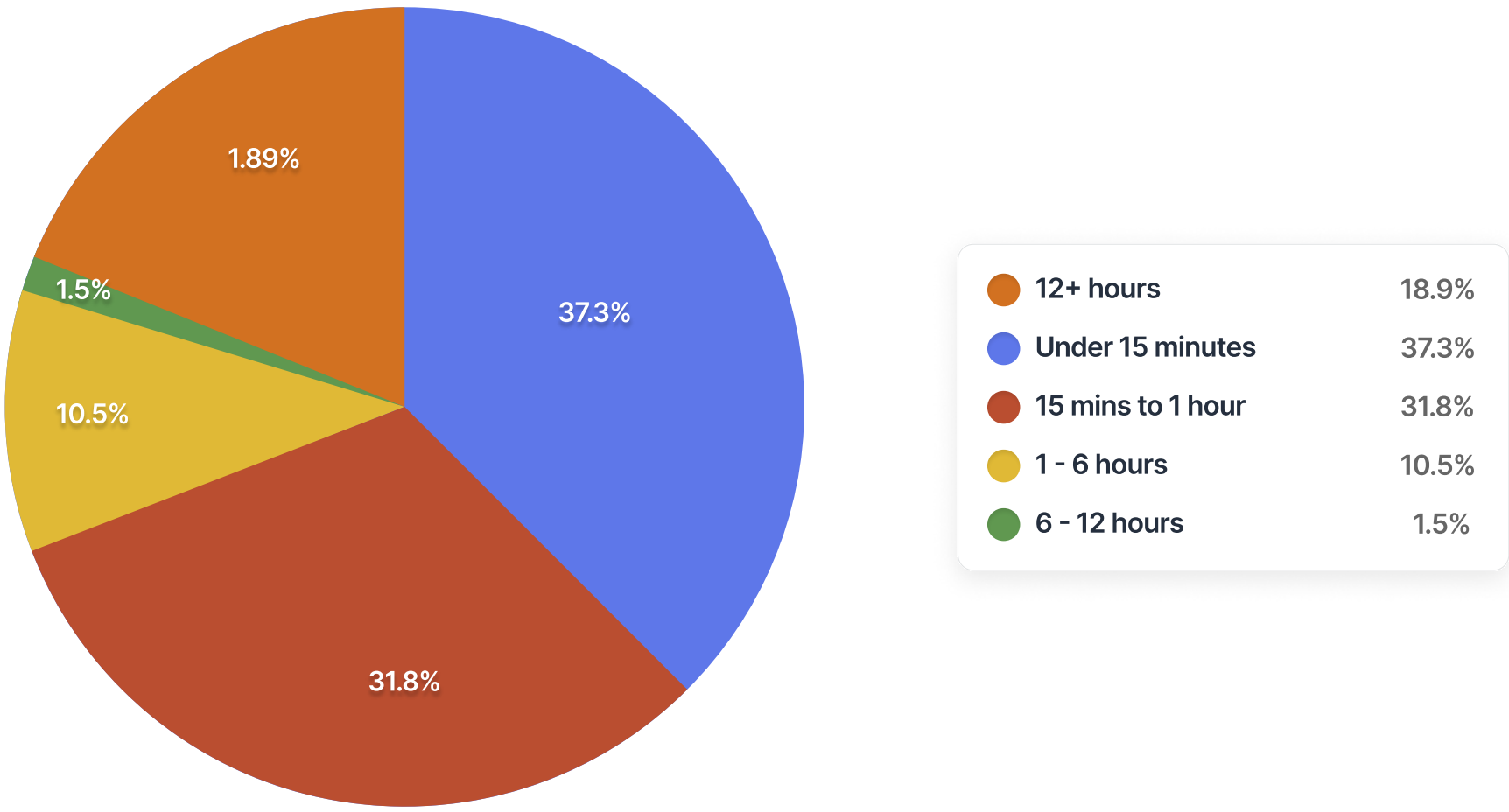
Throughout the course of the day the company was hit by several DDoS attacks on multiple sites, and the onslaught lasted several days. The hackers applied sophisticated tactics to avert mitigation, such as constantly changing attack vectors and ransom note methods. Despite the changing attack patterns, Imperva successfully mitigated the attacks within seconds using mainly threat intelligence, as the sources were known to us as malicious; and bot protection, as the clients were impersonating a legitimate browser or Googlebot.

18%+ of attacks lasted more than 12 hours

Of DDoS attacks mitigated in Q1, **40%** of all attacks were quite short, under 15 minutes in duration; however, almost **20%** of all application layer DDoS attacks during Q1 lasted 12 hours or more.

Under 15 minutes	37.3%
15 mins to 1 hour	31.8%
1 - 6 hours	10.5%
6 - 12 hours	1.5%
12+ hours	**18.9%**

[1] It is not clear whether the threats were really made by the original REvil group or by an imposter.



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 attack no matter the size or the duration with most attacks mitigated in under one second.

Also interesting is that almost **90%** of all DDoS attacks in the same period were between 1,000 and 10,000 Requests per Second (RPS). Shorter and smaller attacks are more likely to fall under the radar and slip through the security net, depending on how effective your DDoS mitigation is.

Prolonged/Sustained DDoS attacks can severely hamper your website's performance; limit site availability; or in the worst case scenario, even take your site offline.

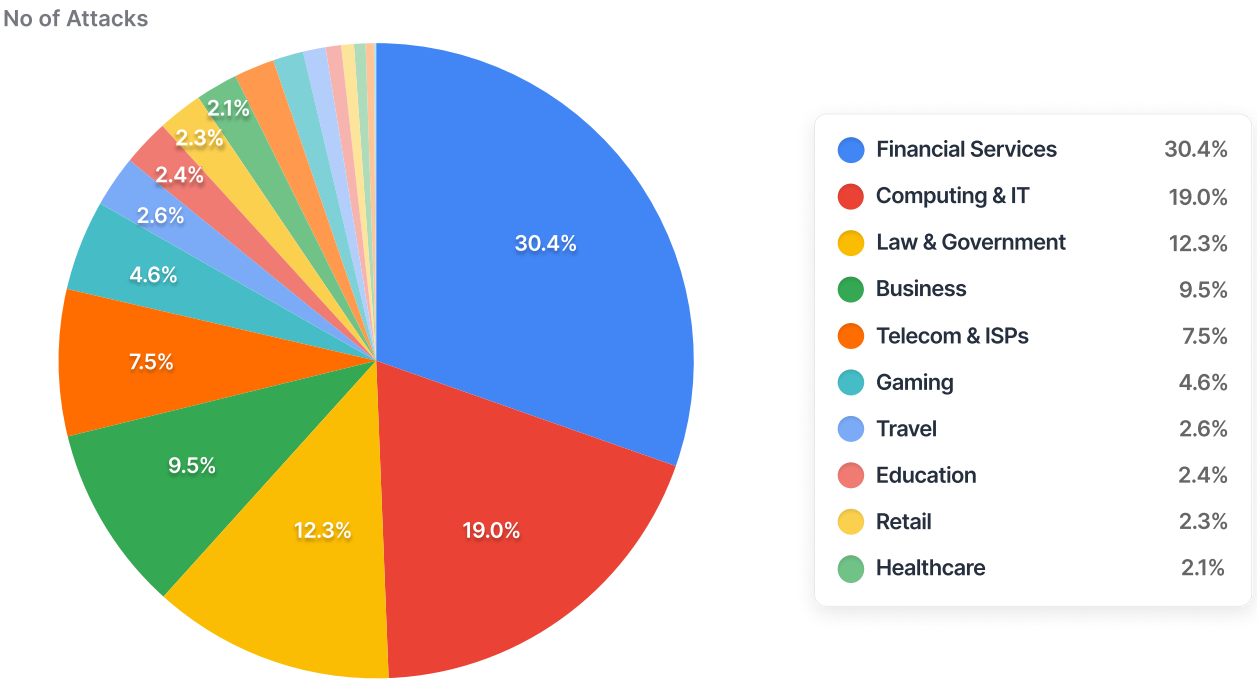
Targeted once and you're likely to be targeted again

Over **50%** of sites hit by a DDoS attack during Q1 were targeted again. This would infer that If you are attacked once you are likely to be attacked again, dispelling the myth that if you have already been the target of a DDoS attack it is unlikely to happen again.

Over 30% of all attacks targeted Financial Services

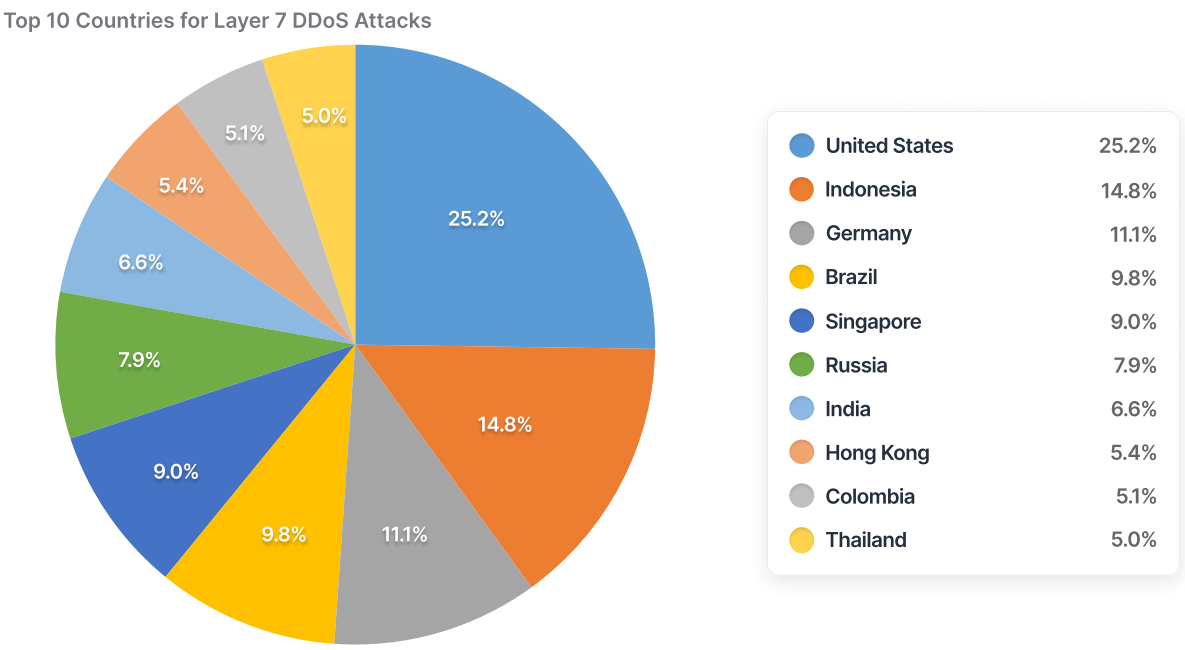
Financial Services still remains the most targeted industry with over **30%** of all Layer 7 DDoS attacks impacting this sector. As more and more financial transactions are executed online, cybercriminals strive to find new and innovative ways to disrupt and corrupt this highly lucrative sector, whether for financial gain or pure cyber vandalism motives. Looking at all industries, around half of all attacks in Q1 targeted either Financial Services or the Computing and IT industries. Interestingly, the Legal and Government sectors have surpassed popular target industries like Gaming and Telecoms, experiencing more than **13%** of all Layer 7 attacks mitigated by Imperva in Q1.

The chart below shows the percentage of DDoS attacks per industry. Learn more about Protecting Financial Institutions from DDoS attacks in our white paper on the subject.



Layer 7 Attacks - Top Source Countries

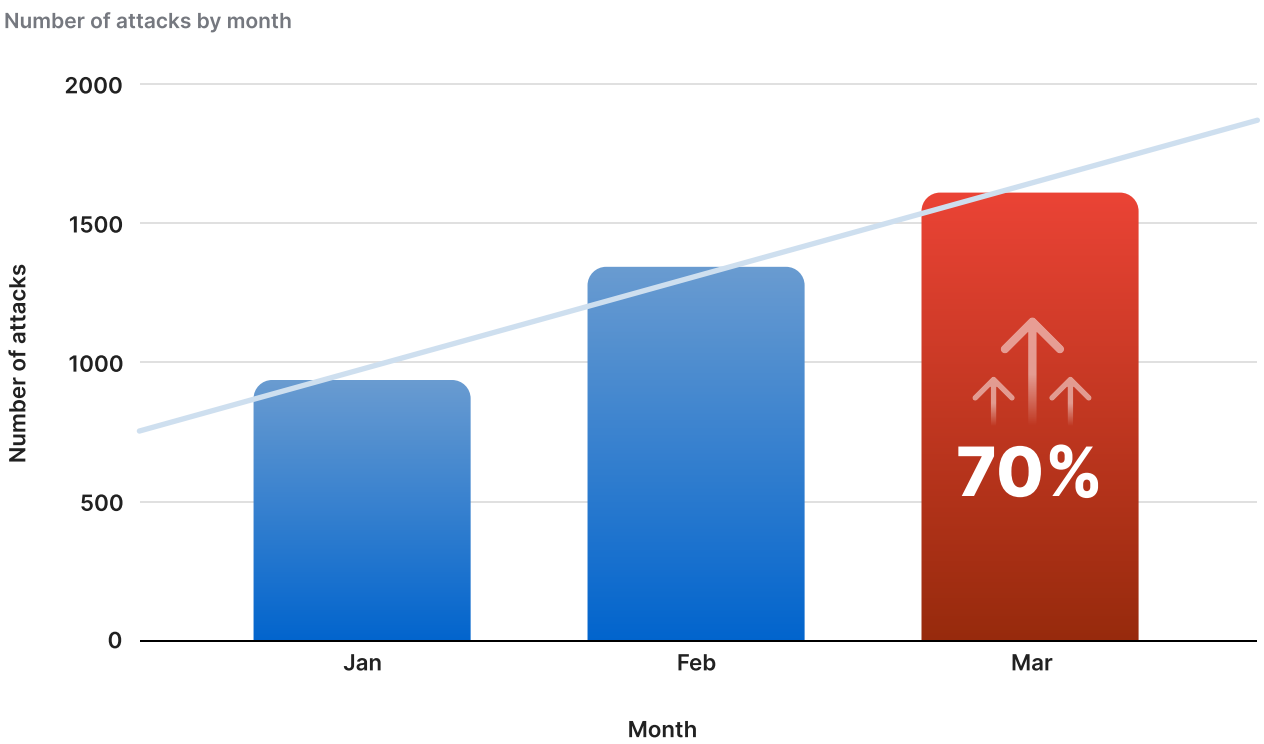
The chart below shows the top source countries ranked by number of requests issued between January and March 2022. Russia is in the top 10 countries as the source for almost **8%** of all Layer 7 DDoS attacks mitigated by Imperva in Q1; however, a higher number of attacks originated in Singapore, Brazil, Germany, and Indonesia, with the United States at top of the list as the source country for over a quarter of all Layer 7 DDoS attacks mitigated.



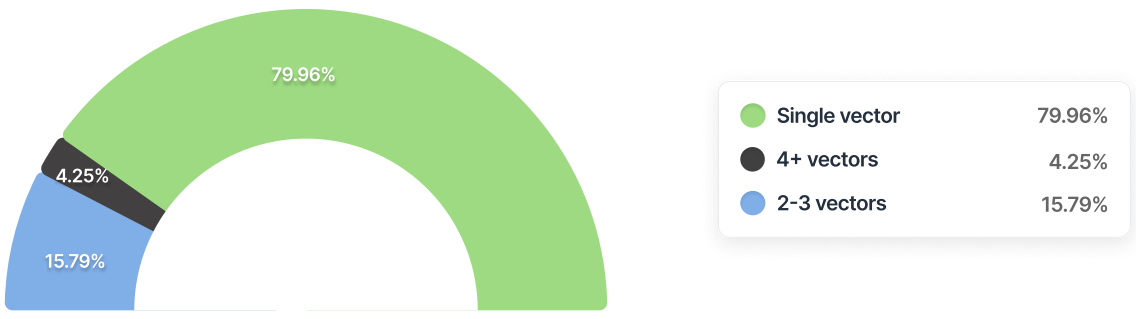
Layers 3 and 4 DDoS attacks

The number of DDoS attacks increased by 70% in March

The overall number of Layer 3 and 4 DDoS attacks almost doubled between January and March 2022 with an increase of **70%**. Global events and a higher volume of cyber warfare attacks are possible contributory factors to this Q1 spike.



Multi-vector attacks became less common

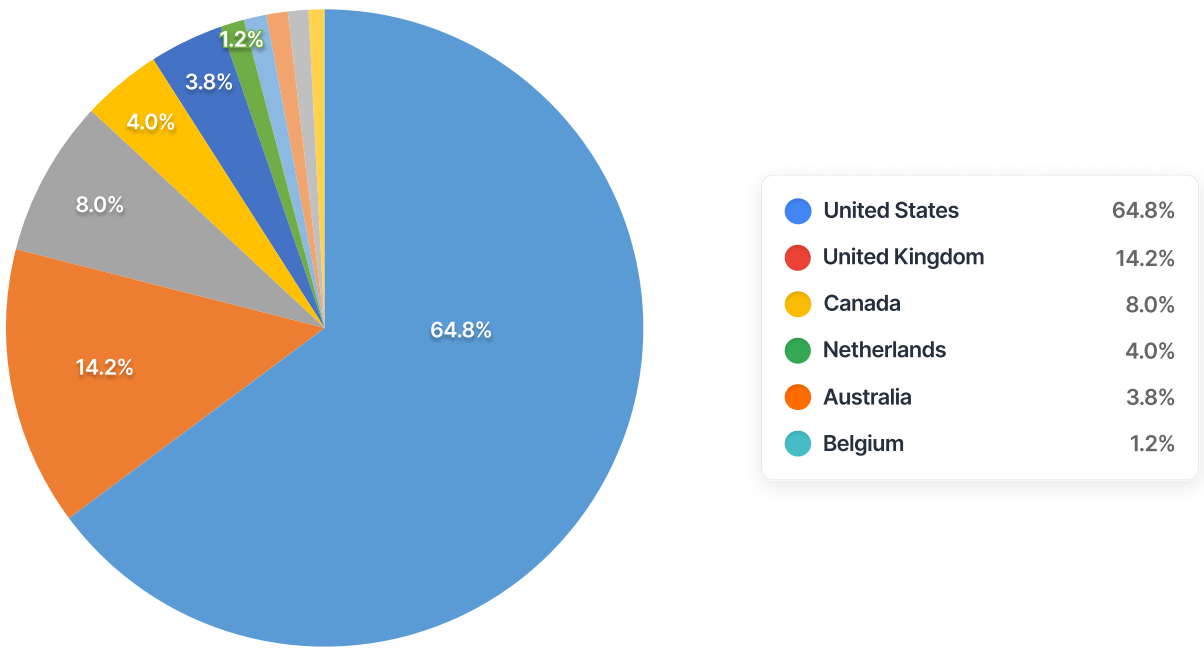


This trend doesn't rule out new vectors emerging. On the contrary, we have observed two new and dangerous DDoS attack vectors in the first three months of the year.

New attack vectors

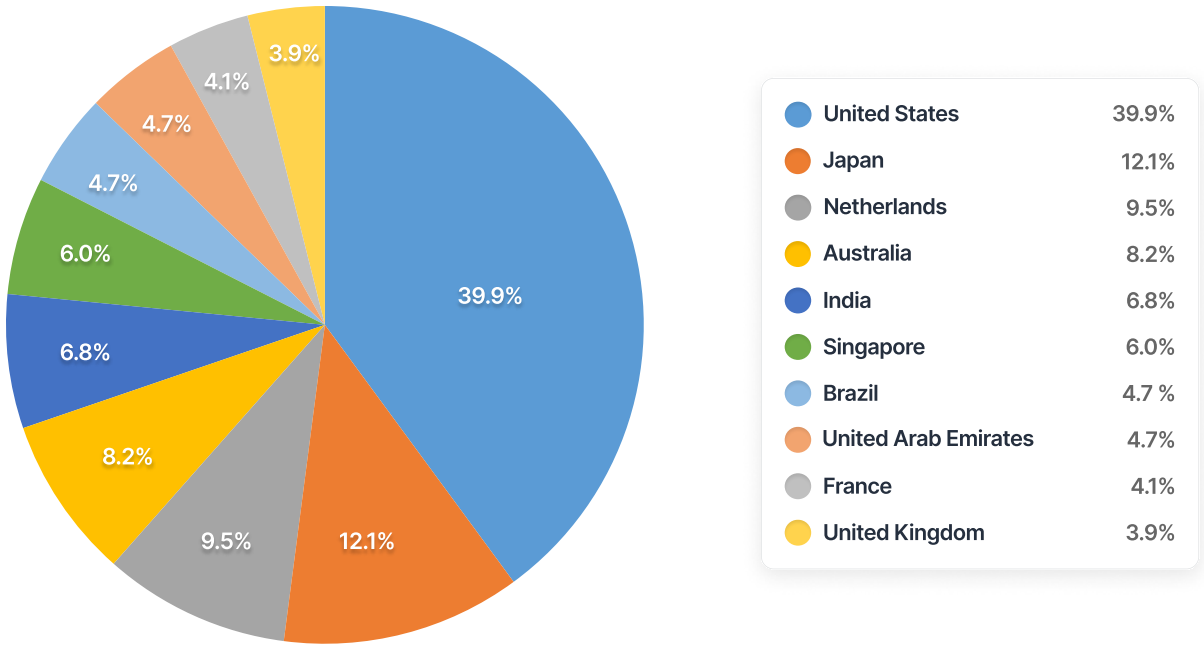
Since the beginning of this year we have seen new vectors emerging, including a new reflection/amplification DDoS vector TP240PhoneHome, first observed by researchers in February, where attackers abused a large number of TP-240 VoIP-processing systems to launch multiple high-impact attacks.

UDP TP240 Attacks - Top 10 Source Countries



Also in Q1 another new attack vector was observed in attacks mitigated by Imperva. 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.

TCP Middlebox Amplification Attacks - Top 10 Source Countries

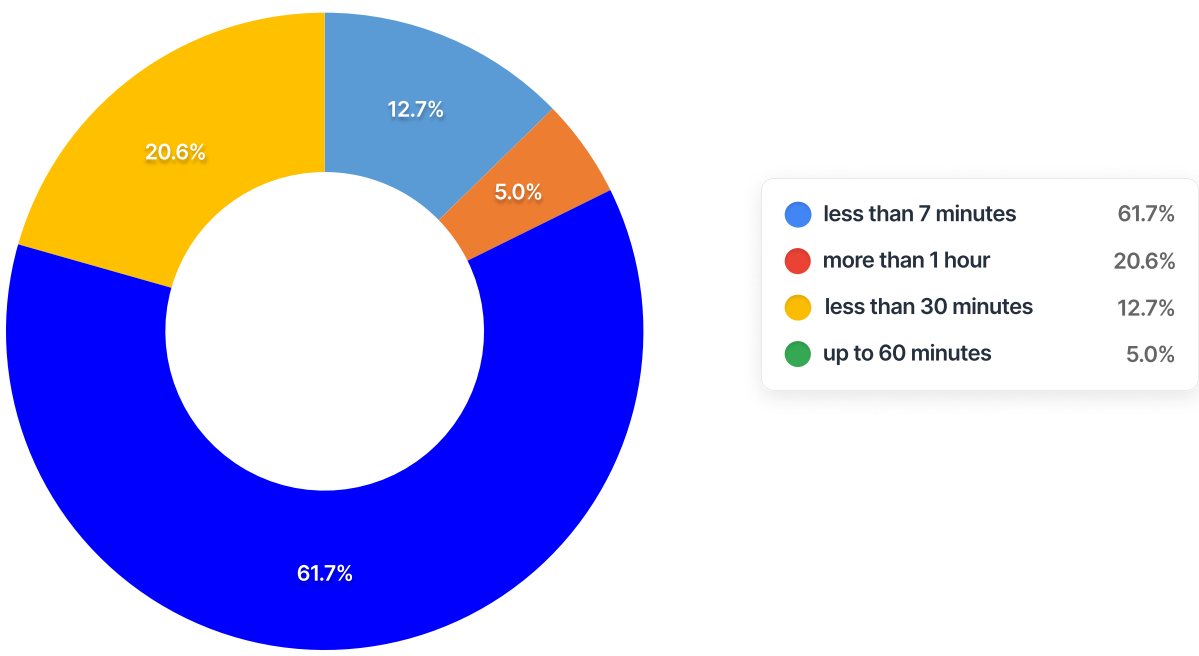


In TCP middlebox amplification attacks, attackers leverage a new amplification technique called TCP Middlebox Reflection leveraging non-compliant TCP middlebox servers to induce them to respond and amplify network traffic against their victims.

Attack duration was shorter

Layer 3 and 4 DDoS attacks reduced in duration during Q1, emphasising the importance of TTM (time to mitigation) and the benefit of having a strong, guaranteed SLA to ensure that your DDoS mitigation will be effective against all types of attacks, no matter how short.

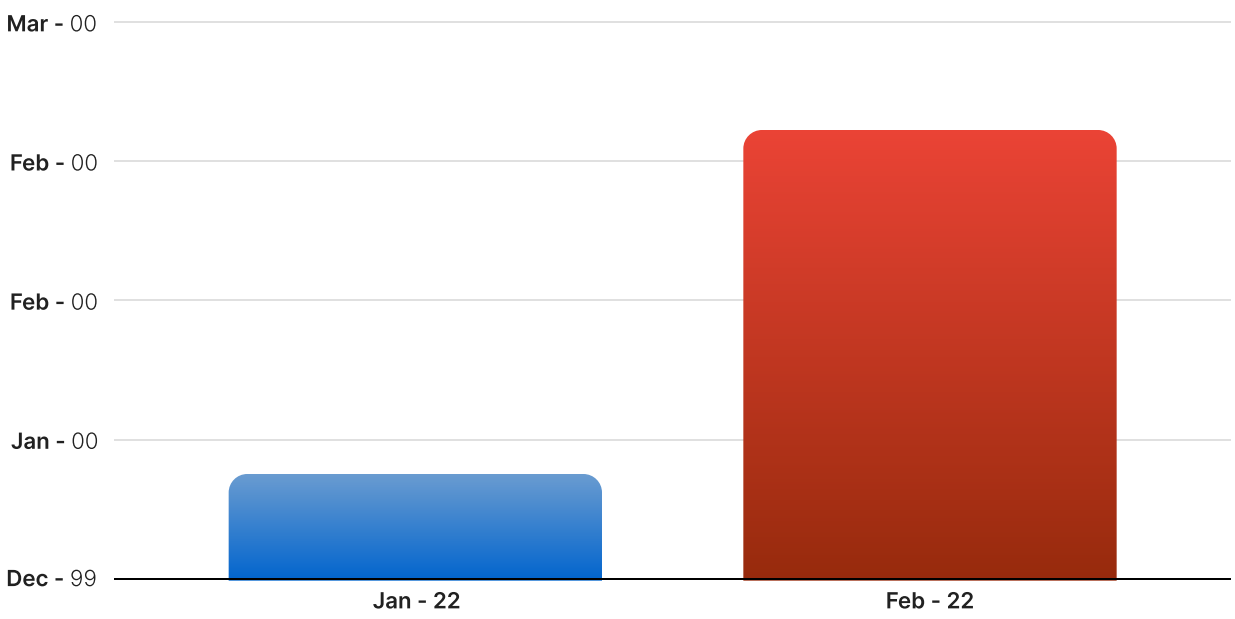
Attack Duration



Attacks on websites in Ukraine and Russia increased by 320%

We saw a X 4 increase in Layers 3 and 4 DDoS attacks on Ukrainian and Russian websites from January to February 2022. The sharp rise in attacks on sites in these conflicting countries is demonstrative of cyberwarfare picking up pace alongside geo-political unrest around the world. Many of the attacks contained messaging targeted in Russian towards the target nation.

Increase in Layers 3 and 4 Attacks on Russian and Ukrainian targets



Have you experienced an attack? Contact Imperva

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. This type of attack consumes actual server resources, or those of intermediate communication equipment such as firewalls and load balancers, and is measured in packets per second (Pps).

Ransom DDoS Attack

A ransom DDoS attack is an extortion-based threat, motivated by the simplicity of carrying out a DDoS attack and the promise of easy, low-risk financial gain. Attackers often send an email demanding payment, often in Bitcoin, to avoid being hit by a DDoS attack. This is often followed by a short attack launched to prove they mean business.

Further definitions of DDoS attack types can be found here.