imperva | Research Labs

REPORT | 2020

DDoS Attacks in the Time of COVID-19

Contents

ABOUT THE REPORT

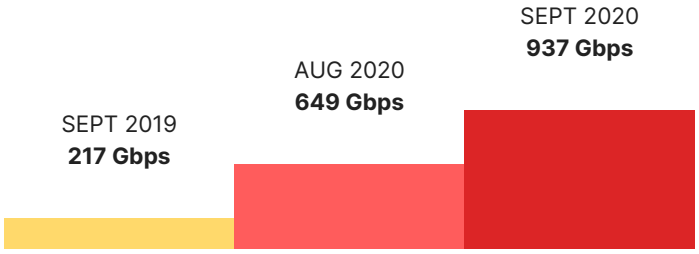
This report provides an understanding of DDoS-related activity and security concerns as observed by Imperva Research Labs during the COVID-19 pandemic[1] period. While the DDoS threat has always been present, the COVID-19 era has seen changes in the attack landscape.

[1]The comparative sections of this report look at a 12 month period spanning the 6 months prior to March 2020 and the 6 months after. All data has been provided by Imperva Research Labs.

DDoS attacks bigger than ever

Attacks are growing over time

Large attacks ranged from 217 Gbps in September 2019, followed by a 649 Gbps attack in Aug 2020, and a 937 Gbps attack in September 2020.



Network DDoS traffic increased by 24%

Network DDoS traffic has increased by 24%. We also observed a 41% increase in the total number of DDoS packets and a 21% increase in DDoS attack duration.

24% ▲ Network DDoS Traffic

41% ▲ DDoS Packets

21% ▲ Attack Duration

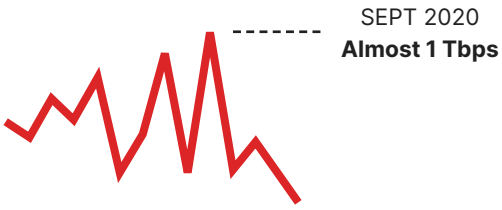
Application DDoS attacks increased in intensity by almost 80%

The maximum Requests per Second (RPS) of application DDoS attacks increased significantly in the 12 months between September 2019 and August 2020.

80% ▲

Imperva mitigated its largest attack to date

In September 2020 we mitigated an intense DDoS attack that peaked at almost 1 Terabit per second (Tbps).



COVID-19 trends affecting cyber security

2020 has been a year of unprecedented change and uncertainty for business due to the COVID-19 pandemic. However, one constant always remains and that's the threat of a cyber security attack on businesses. Imperva Research Labs has been monitoring DDoS trends over a 12 month period spanning the six months prior to March 2020 and the six months after, when the effects of the pandemic on businesses really began to take hold.

Increased online activity

For cyber attackers, the most significant changes were COVID-19 lockdown restrictions and the shift to remote working. In the early part of the year, organizations and workforces had to quickly adapt to remote working on a massive scale. With sheltering in place restrictions being imposed in many countries around the world, millions of people turned to the internet to meet their work, retail, and recreational needs. This shift in online activity created a surge in internet traffic that substantially expanded the scope for attacks.

Targeted industries

Comparing the two periods[2], Imperva's research shows that DDoS attacks on certain industries have increased significantly including;

CATEGORY	CHANGE
Automobile	**+ 108%**
Telecommunications / Internet Service Providers	**+ 53%**
Marketing	**+ 43%**
Gambling	**+ 32%**
Financial Services	**+ 30%**

However other industries such as Retail experienced an upsurge of attacks at certain times during the COVID months most likely due to increased online traffic volumes.

Attack magnitude almost doubled

While there hasn't been an increase in the number Application DDoS attacks since March 2020, Imperva's data highlights that the intensity of this type of attack has almost doubled.

Network DDoS attack metrics have increased across the board including traffic volume, attack duration, and packets per second.

[2] Sept 19-Feb 20 vs Mar 20-Aug 20

DDoS attack size reaches new record

In 2019, Imperva reported that we had mitigated our biggest ever attack. This trend for larger attack sizes has continued throughout the COVID pandemic, with a number of unprecedentedly large DDoS attacks taking place between July and September 2020, the most recent of which peaked at almost 1 Tbps.

Remote working challenges

In the early part of 2020, organizations and workforces had to quickly adapt to remote working[3] on a massive scale, a move which substantially expanded the threat surface for attackers. As more and more people turned to the internet to meet their work, retail, and recreational needs, it had never been more important for businesses to ensure uninterrupted online service for their customers.

Remote working raised a number of operational and security challenges for companies. In particular, the soaring internet traffic volumes introduced a new risk that threatened to overwhelm remote security teams who may have found it difficult to distinguish between a legitimate increase in traffic and a DDoS attack.

REMOTE WORKING CHALLENGES FOR COMPANIES INCLUDE:

- Continuous connectivity
- Scaling technology
- Communications
- Dispersed security teams
- Distractions to workers

Network layer attacks

Imperva sensors have seen increases in all categories of layer 3 and 4 DDoS attacks.

Network DDoS traffic volumes increased by 24% with attack duration rising by 21%. The most significant increase for this attack type was in the number of packets, which grew by 41% in the previous six months.

CATEGORY	CHANGE
Network DDoS traffic volume	+ 24%
Attack duration	+ 21%
Number of packets per second	+ 41%

41%

INCREASE IN PACKETS PER SECOND

These changes indicate a more sophisticated style of DDoS attack where the attacker aims to overwhelm switch resources as well as achieving the volumes needed to impact available bandwidth. DDoS protection should have not only the capacity to absorb attacks in terms of bandwidth, but also the deployment capacity to handle millions of packets per second to prevent downtime.

[3] Surge in online traffic increases risk to businesses

Application layer attacks

79%

INCREASE IN MAX RPS FOR APPLICATION DDOS ATTACKS

While Imperva's data doesn't show a marked difference in the number of application layer DDoS attacks since March 2020, it highlights another remarkable trend — an increase in the intensity of attacks. Intensity is measured by the number of requests per second (RPS) made during a DDoS attack.

The research shows that the maximum RPS of application DDoS attacks grew by 79% compared to the previous six months, meaning these attacks have almost doubled in intensity during the pandemic period.

Larger and more sophisticated attacks

Imperva Research Labs recorded two large DDoS attacks in July 2020. In keeping with the most targeted industries during the pandemic period, the first of these attacks was an application layer attack on a 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.

Attack 1 - Application Layer Attack

INDUSTRY	Gambling
NUMBER OF SOURCE IPS	851
DURATION	<10 mins
SIZE	689,000 RPS

The second attack observed was a massive network layer attack against a single target in India. Reaching 398 Gbps, the attack consisted of a syn flood (76% of its packets were between 0 and 100 bytes), reinforced by a second, larger syn flood (24% of its packets were between 100 and 900 bytes).

Attack 2 - Network Layer Attack

SIZE	398 Gbps
SYN FLOOD 1	76% of packets between 0-100 bytes
SYN FLOOD 2	24% of packets between 100-900 bytes

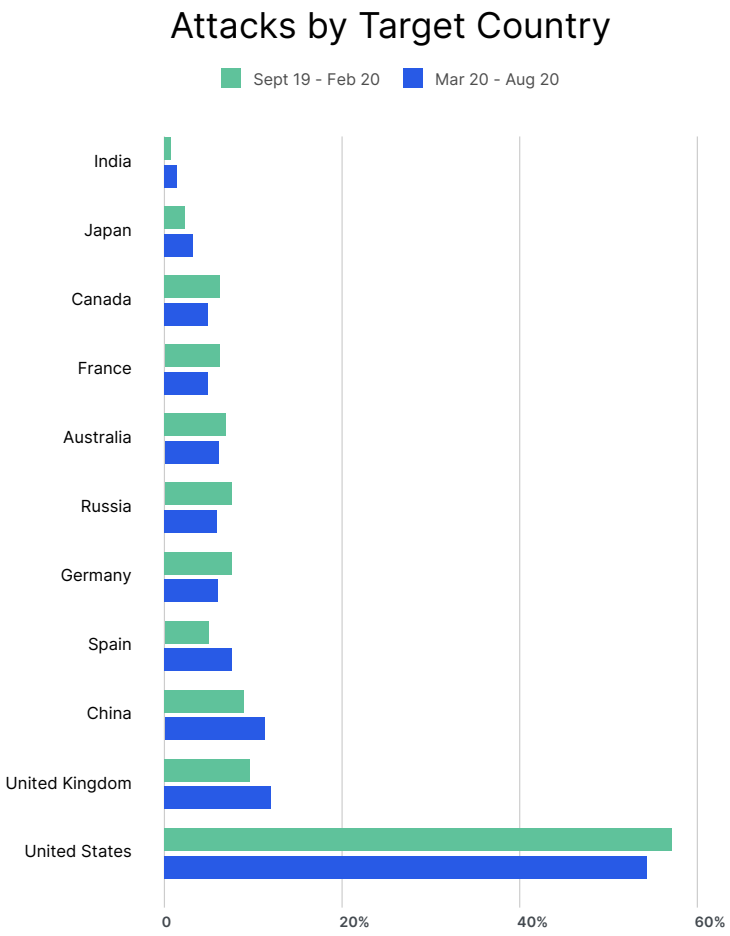
Both attacks were unprecedented in terms of their size and intensity, and were indicative of the increasing recurrence of larger and more sophisticated application DDoS attacks.

September saw a further rise in the number of DDoS attacks where both the volume of attacks and their level of intensity increased significantly. One such attack peaked at nearly 1Tbps, breaking Imperva's record to date.

This attack[4] was more sophisticated in its approach as the attackers combined two separate vectors, large SYN and TCP, which they leveraged in two waves. The first consisted of a 90 second burst of large SYN flood – basically a SYN flood with a large payload followed by a TCP flood which attempted to mimic the customer's legitimate traffic, making it more difficult to mitigate. This initial burst was so powerful, it peaked at 674Gbps and 148Mpps in under five seconds, emphasising how important it is to start DDoS mitigation within seconds of an attack.

DDoS attacks by target country

As you can see from the chart, the countries most targeted changed very little prior to and during the pandemic, with the United States and the United Kingdom easily occupying the top two positions.



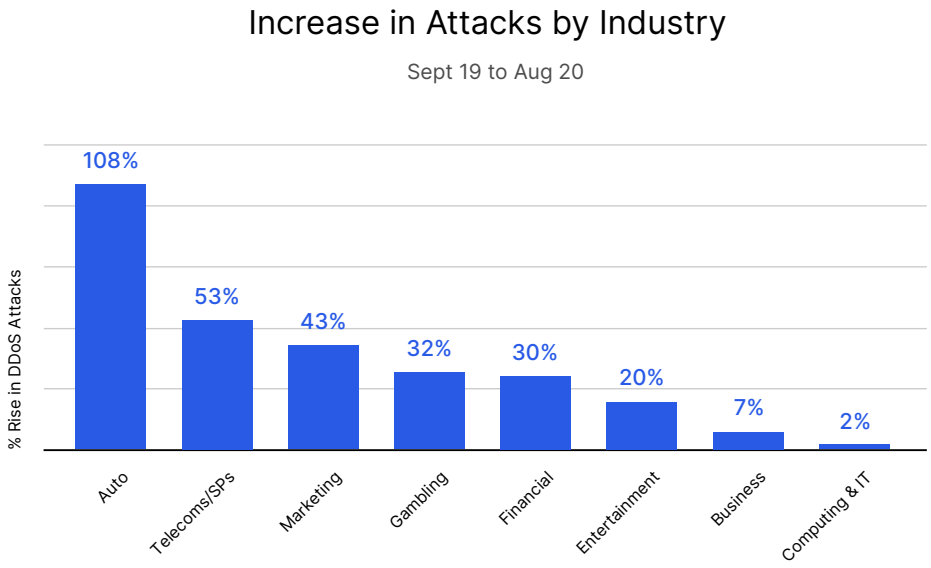
[4] DDoS Attacks Grow More Sophisticated as Imperva Mitigates Largest Attack

Attacks by industry

Since March 2020, we've seen an increase in application DDoS attacks in certain industries[5]. Imperva's data shows that, in this timeframe, the industries showing the most growth are:

53%

INCREASE IN ATTACKS ON TELECOM SERVICE PROVIDERS



It's important to remember that our research is based on DDoS attacks on Imperva customers only and that the figures do not necessarily reflect universal DDoS attack trends per industry.

See our latest Cyber Threat Index (CTI) Report for a more in-depth analysis of the global cyber threat landscape looking at attacks by type, industry, and by country. The report also provides a monthly easy-to-understand score to track the cyber threat level consistently over time as well as observe trends.

As you would expect the Retail sector experienced a spike in DDoS attacks in April at the height of lockdown in many locations.For a more detailed review of this sector Imperva has recently published a report: The State of Security within eCommerce.

[5] New Cyber Threat Index Shows Industries Are Under Attack in Uncertain Times

Return of ransom DDoS attacks

In September, an old attack type made a comeback: a major global Ransom Denial of Service (RDoS) campaign[6] mainly targeting financial services organizations.

RDoS campaigns are extortion-based DDoS threats motivated by financial gain and demanding payment in bitcoin currency to prevent a DDoS attack on their target's network. In this case, the extortionists claimed a connection to infamous Advanced Persistent Threat groups such as Fancy Bear and Lazarus Group.

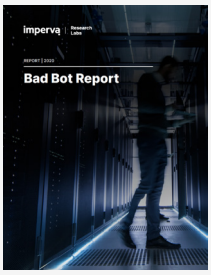
The campaign consisted of an email threat to launch a DDoS attack against the target's entire network if the demanded ransom wasn't paid within six days. The threat stipulated that, once the attack had started, only a payment of 30 bitcoin (approx USD $328K) would be able to stop it, with an additional 10 bitcoin (USD $110K) demanded for each day the ransom remained unpaid. The extortionists also threatened to begin a small DDoS attack on the company's main IP address immediately to prove the threat was genuine.

DDoS attacks don't always come with a ransom demand but, given that even one hour of downtime can cost organizations up to $100K, this type of RDoS attack is worth taking seriously and mitigating against.

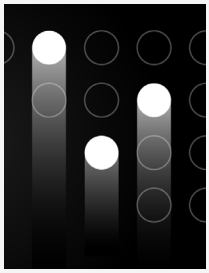
Fortunately Imperva was able to mitigate these attacks on behalf of our customers but this is a reminder of how your business is at an advantage if you have strong DDoS protection in place.

Further reading

2019 GLOBAL DDOS THREAT LANDSCAPE REPORT



BAD BOT REPORT 2020: BAD BOTS STRIKE BACK



IMPERVA CYBER THREAT INDEX REPORT

THE STATE OF SECURITY WITHIN E-COMMERCE REPORT

[6] Major Global Ransom Denial of Service Campaign Continues Rising Trend in Global DDoS Attacks

About Imperva Research Labs

Imperva Research Labs is a premier research organization for security analysis, vulnerability discovery and compliance expertise. The organization provides round-the-clock research into the latest security vulnerabilities and is comprised of some of the world's leading experts in data and application security. Imperva Research Labs combines extensive lab work with hands-on testing in real world environments to ensure that Imperva's products, through advanced data and application security technology, deliver up-to-date threat protection and unparalleled compliance automation. Incorporating exceptional insight, Imperva Research Labs publishes reports on a quarterly basis like the Global DDoS Threat Landscape Report and Bad Bot Report that provide insight and guidance on the latest security threats and how to mitigate them.

WHAT'S NEXT

For more information about Imperva DDoS protection services, **visit our website.**

And, visit the DDoS Mitigation section of our Resource Library for more DDoS-related content.

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.