TATA COMMUNICATIONS

TATA

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

CISO DDoS HANDBOOK

Get ahead or get taken down – the proactive steps you need to protect your business from DDoS attacks

2022

INDEX

01
The basics of DDoS attacks

02
Motivations for DDoS attacks

03
The rapid increase in DDoS attack volumes

04
DDoS attacks - inexpensive and easy to launch

05
DDoS attacks - can cost businesses a fortune

06
Four key ways to protect your business

07
Factors to consider while choosing a DDoS protection provider

08
Explore Tata Communications' DDoS Protection Services

The evolving cyberattack landscape

A business's digital presence is now one of the most critical factors in its success. To attract and retain customers, companies must provide a fast, effortless and engaging online experience. In addition, customers' data and transactions must be secure. However, as the world increasingly moves online, businesses and individuals are at greater risk of cyberattacks.

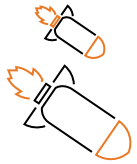
Distributed Denial of Service (DDoS) attacks are slowly becoming one of the biggest concerns for CISOs worldwide. According to a recent study[1], 30 percent of CISOs consider DDoS attacks one of their organisation's most significant cyber threats. It is crucial to better understand the trends, motivations, and costs involved to protect ourselves against today's DDoS attacks.

30% of CISOs consider DDoS attacks one of their organisation's most significant cyber threats.

The basics of DDoS attacks

DDoS, or 'Distributed Denial of Service', is a cyberattack in which the attacker seeks to make an online service unavailable by overwhelming it with internet traffic from multiple sources. DDoS attacks are often carried out by botnets or networks of infected computers that can be controlled remotely by the attacker. The attacker sends commands to the botnet, instructing it to send large amounts of data to the target server over a short period of time. This generally overloads the server and causes it to crash or become unresponsive. DDoS attacks can be difficult to defend against because they can come from anywhere and use many devices. As a result, DDoS attacks can be disruptive and cause significant financial damage.

There are multiple types of DDoS attacks, each with its distinct purpose and method. The most common type of attack is the volume-based attack, which attempts to flood the target with traffic, overwhelming its ability to process requests. Another common type is the protocol-based attack, which targets a specific component of the network protocol stack, such as the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). Finally, there are application layer attacks, which target specific applications or services running on a server. These attacks can be especially challenging to mitigate, as traditional security measures may not detect them.



DDoS attacks can be difficult to defend against because they can come from anywhere and use many devices.

Motivations for DDoS attacks

Attackers often try to extort money from businesses by threatening to launch a DDoS attack unless a ransom is paid. In other cases, non-financial motivations such as political protests may be the driving force behind an attack. Hacktivists, for example, have been known to launch DDoS attacks to draw attention to their cause. Additionally, DDoS attacks are often used as a smokescreen for other targeted attacks. By overwhelming the target system with requests, incident response teams may be distracted from more significant breaches that are taking place. Finally, state-sponsored groups sometimes carry out DDoS attacks as part of a more extensive cyberwar campaign. These attacks typically target government organisations or critical infrastructure organisations in another country.

While DDoS attacks can be launched for a variety of reasons, the most common motivations are **financial gain, hacktivism, and cyberwarfare.**

The rapid increase in DDoS attack volumes

DDoS attacks are becoming more common. According to a new report, DDoS attacks reached an all-time high in Q1 2022 compared to the previous year.

DDoS attacks are also becoming increasingly powerful. The average DDoS session in Q1 2022 lasted 80 times longer than in Q1 2021, with the longest episode lasting 549 hours (nearly 23 days).[3] This means that enterprises need to strengthen their IT vigilance and make sure they are well prepared to counter malicious denial of service attacks.

Recently, an American video game company was hit by a DDoS attack, resulting in high latency and disconnection for some players. A series of DDoS attacks targeted several public websites managed by state entities across the world, including Romania, Iceland, and Finland.

DDoS attackers are **increasing by 450 percent** year on year and by **46 percent** compared to the previous quarter.[2]

DDoS attacks - inexpensive and easy to launch

It's challenging to hack a server or website. But it's much simpler to launch DDoS attacks, given that servers have a limit on how much traffic they can handle.

Due to the rise in DDoS-for-hire services, DDoS attacks are now easier to carry out than ever before. Numerous DDoS-for-hire service providers in the deep and dark web provide flexible payment options based on the attack's setup, length, throughput and bandwidth. Some providers even offer free trials, while others may charge a nominal $5 price over a five-day trial period. It costs $6,500 to launch 100 concurrent attacks, with no daily limits and a committed 1 million packets per second (Mpps)[4].

DDoS attacks - can cost businesses a fortune

When an organisation's systems are down, employees are unable to work, and customers are unable to access services. One hour of downtime that causes mission-critical server hardware and apps to go down costs an average of nearly $300,000 in lost revenue, productivity disruptions, and remediation efforts, according to a 2021 study. So, the longer the duration of a DDoS attack, the more significant its adverse effects[5].

In addition, DDoS attacks can damage a business's reputation and result in higher insurance premiums. These costs can add up quickly, making DDoS attacks a very costly form of cybercrime. The DDoS attack that resulted in several days of disruption for a well-known international VoIP service provider is a real-world illustration of the consequences of a DDoS attack. It significantly damaged the company with an earnings loss of between $9 million and $12 million in just one quarter.

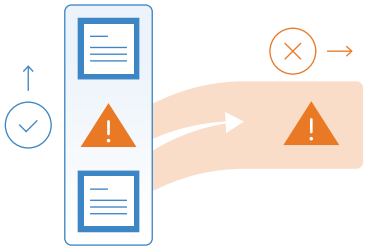
An hour of server downtime can lead to losses of nearly **$300,000**

Four key ways to protect your business

DDoS attacks are becoming more powerful, sophisticated, and challenging to defend against. Enterprises must be vigilant and take steps to prepare for these malicious attacks. Some of the critical measures that enterprises can take include:

01 Keep up to date with the latest tactics used by attackers

In today's digital age, it is more important than ever to be aware of the latest DDoS attacks and how to protect against them. As technology evolves, so do the techniques used by attackers. That's why it's critical to stay up-to-date with the latest DDoS threats and prepare a network to handle them.



02 Look for ways to reduce the potential attack surface

One way to mitigate DDoS attacks is to minimise the exposure of applications or resources to ports and protocols that aren't expecting any communication.

03 Plan for higher traffic volumes

This can be accomplished by running on more extensive computation resources or features such as more extensive network interfaces or enhanced networking that support higher volumes. Additionally, load balancers are commonly used to continuously monitor and shift loads between resources to avoid overloading any single resource.

04 Consider partnering with DDoS protection experts

You will need the right tools and know-how to detect a DDoS attack and intelligently drop malicious traffic, and make the rest of the traffic available to your users. This entails purchasing and maintaining costly equipment and having a network capable of absorbing attacks. Instead, consider approaching DDoS protection experts for help and support.

Stay up to date on latest threats with our threat advisory.

Factors to consider while choosing a DDoS protection provider

A DDoS protection service can help to mitigate the impact of DDoS attacks, but it is crucial to choose the right service for your needs. When considering a DDoS service provider, you should ask a few key questions to determine if they are the right fit for your organisation.

Let's take a closer look at the criteria you can use to choose a DDoS protection service.

Do they have enough network capacity?

When considering a DDoS protection solution, be sure to inquire about the provider's network capacity. It's a good indicator of how well they'll handle even the largest attacks and whether they have enough capacity to handle multiple attacks simultaneously. A 10 Tbps (terabits per second) network can theoretically block up to the same volume of attack traffic, minus the bandwidth required to maintain its regular operations. Most cloud-based mitigation services offer multi-Tbps network capacity – beyond what you might ever need. On-premise DDoS mitigation appliances, conversely, are capped by default – both by the size of an organisation's network pipe and the internal hardware capacity.

Most cloud-based mitigation services offer multi-tbps network capacity

How long do they take to mitigate attacks?

Time to mitigation is critical when you're under DDoS attack. You'll want to determine how quickly the DDoS protection provider can identify and block an attack. This is important because the sooner an attack is detected, the less damage it will cause. Make sure test beds are available to run tests before committing them to production.

You'll want to determine how quickly the DDoS protection provider can identify and block an attack

Can they offer low latency for a better user experience?

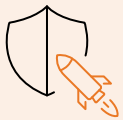
It is critical to understand that legitimate traffic will pass through the network of your DDoS protection provider at some point. You require a service that ensures optimal connectivity between your data centre and users. They should ideally have Points of Presence (PoPs) near their end users. This is very important. Assume that most of your customers are in India, and you use a DDoS protection service with PoPs only in Japan. Every user request will be routed to the Japanese PoP, then to your data centre in India, back to the Japanese PoP, and finally to the user. The result is multi-fold latency, leading to a poor end-user experience.

It's vital your provider has PoPs near their end users

Factors to consider while choosing a DDoS protection provider

A DDoS protection service can help to mitigate the impact of DDoS attacks, but it is crucial to choose the right service for your needs. When considering a DDoS service provider, you should ask a few key questions to determine if they are the right fit for your organisation.

Let's take a closer look at the criteria you can use to choose a DDoS protection service.



Can they protect against a variety of DDoS attacks?

When it comes to DDoS protection, there is no one-size-fits-all solution. So, the best way to ensure comprehensive coverage is to choose a solution that offers protection against different types of attack. Volumetric attacks, for example, are designed to overwhelm the bandwidth of a target system. On the other hand, application-layer attacks exploit vulnerabilities in a target system's application layer. And SSL/TLS floods target the SSL/TLS encryption protocol to overload a target system. There are also new types of DDoS attacks, such as low-rate attacks, which are difficult to distinguish from legitimate traffic, multi-modal attacks that launch several different types of DDoS attacks simultaneously, and WS-Discovery attacks that allow unauthenticated traffic to pass through and amplify attacks.

By choosing a DDoS solution that offers protection against a variety of attacks, you can be confident that your systems will be safe from even the most sophisticated threats.

Choose a solution that offers protection against a variety of DDoS attacks

What's their track record in this area?

When choosing a DDoS protection service, the experience and expertise of the provider are essential factors to consider. An experienced provider is likely to have a deep understanding of the challenges of protecting against DDoS attacks. Their invaluable knowledge and experience, developed over the course of thousands of projects, will enable them to identify and implement best practices. So, when assessing providers, ask about their track record.

An experienced provider will understand the challenges of protecting against DDoS attacks

Read how **Tata Communications helped a major Indian bank mitigate a targeted DDoS attack and fine tune its protection policies to protect against future attacks.**

In conclusion

Today's digitally-literate consumers are savvy and have high expectations. They are used to having instant access to information and services. If a business cannot provide this, it will quickly lose customers to its competitors. There's no question that there are more DDoS attacks than ever before, and that they are also more powerful and damaging. Enterprises must therefore be vigilant and take steps to partner with the right DDoS protection provider to withstand attacks and keep their business operations running smoothly. All the above factors are vital in ensuring that your DDoS protection is managed successfully.

Explore Tata Communications' DDoS Protection Services

Tata Communications provides advanced DDoS protection to businesses around the world. Regardless of the DDoS attack's volume, complexity or duration, our DDoS protection service offers real-time detection and mitigation with minimal manual intervention. Get in touch and find out how our decade-long experience, massive capacity, and multi-layered protection can help keep your organisation safe from DDoS attacks.

Visit our website to know more about our DDoS protection services.

Sources:

1. CISOs say ransomware is the least concerning threat to enterprises
2. Major DDoS attacks increasing after invasion of Ukraine
3. Report: DDoS attacks have increased 4.5 times since last year
4. DDoS-for-hire attacks cost less than a used car
5. The Cost of Enterprise Downtime