What you need to know about DDoS cyber attacks

According to Arbor Networks' 12th Annual Worldwide Infrastructure Security report, the chances of organisations being hit by a Distributed Denial of Service (DDoS) attack have never been higher.

“DDoS attacks affect more than just IT. They affect business, money and personal lives. It is, however, a technology that is still mostly spoken about in technical terms. We have therefore broken it down into everyday language - as best as possible - so that this daily crime - that has in the past five years shown no means of slowing down - can be understood by all,” says Bryan Hamman, territory manager for sub-Saharan Africa at Arbor Networks.

The basics of DDoS

What is a DDoS attack and how do you protect against this type of attack?

A DDoS attack is an attempt to exhaust the resources available to a network, application or service so that genuine users cannot gain access. Beginning in 2010, and driven in no small part by the rise of Hacktivism, there’s been a renaissance in DDoS attacks that has led to innovation in the areas of tools, targets and techniques.

Today, DDoS has evolved into a series of attacks that include very high volume, yet more subtle and difficult to detect, attacks that target applications as well as existing security infrastructures such as firewalls and IPS.

What are the different types of DDoS attacks?

DDoS attacks vary significantly, and there are thousands of different ways an attack can be carried out (attack vectors), but an attack vector will generally fall into one of three broad categories:

1. Volumetric attacks: Attempt to consume the bandwidth either within the target network/service or between the target network/service and the rest of the internet. These attacks are simply about causing congestion.
2. TCP state-exhaustion attacks: These attacks attempt to consume the connection state tables which are present in many infrastructure components such as load-balancers, firewalls and the application servers themselves. Even high capacity devices capable of maintaining state on millions of connections can be taken down by these attacks.
3. Application layer attacks: These target some aspect of an application or service at Layer-7. These are the most-deadly kind of attacks as they can be very effective with as few as one attacking machine generating a low traffic rate (this makes these attacks very difficult to pro-actively detect and mitigate). These attacks have come to prevalence over the past three or four years and simple application layer flood attacks (HTTP GET flood for instance) have been one of the most common DDoS attacks seen in the wild.

Today's sophisticated attackers are blending volumetric, state exhaustion and application-layer attacks against infrastructure devices all in a single, sustained attack. These attacks are popular because they are difficult to defend against and often highly effective.

The problem doesn't end there. According to Frost & Sullivan, DDoS attacks are innovation "increasingly being utilised as a diversionary tactic for targeted persistent attacks."

Attackers are launching DDoS attacks to distract the network and security teams while simultaneously trying to inject malware into the network with the goal of stealing IP and/or critical customer or financial information.

Why are DDoS attacks so dangerous?

DDoS represents a significant threat to business continuity. As organisations have grown more dependent on the internet and web-based applications and services, availability has become as essential as electricity.

DDoS is not only a threat to retailers, financial services and gaming companies with an obvious need for availability. DDoS attacks also target the mission critical business applications that your organisation relies on to manage daily operations, such as e-mail, salesforce automation, CRM and many others.

Additionally, other industries, such as manufacturing, pharma and healthcare, have internal web properties that the supply chain and other business partners rely on for daily business operations. All of these are targets for today's sophisticated attackers.

What are the consequences of a successful DDoS attack?

When a public-facing website or application is unavailable, that can lead to angry customers, lost revenue and brand damage. When business critical applications become unavailable, operations and productivity grind to a halt. Internal websites that partners rely on means supply chain and production disruption.

A successful DDoS attack also means more attacks. That is, you can expect attacks to continue until more robust defences are deployed.

What are your DDoS protection options?

Given the high profile nature of DDoS attacks, and their potentially devastating consequences, many security vendors have

suddenly started offering DDoS protection solutions.

With so much riding on your decision, it is critical to understand the strengths, and weaknesses of your options.

Existing infrastructure solutions (firewalls, intrusion detection/protection systems, application delivery controllers/load balancers)

IPS devices, firewalls and other security products are essential elements of a layered-defence strategy, but they are designed to solve security problems that are fundamentally different from dedicated DDoS detection and mitigation products.

IPS devices, for example, block break-in attempts that cause data theft. Meanwhile, a firewall acts as policy enforcer to prevent unauthorised access to data. While such security products effectively address “network integrity and confidentiality,” they fail to address a fundamental concern regarding DDoS attacks, “network availability”.

What’s more, IPS devices and firewalls are stateful, inline solutions, which means they are vulnerable to DDoS attacks and often become the targets themselves.

Similar to IDS/IPS and firewalls, ADCs and load balancers have no broader network traffic visibility nor integrated threat intelligence and they are also stateful devices vulnerable state-exhausting attacks. The increase in state-exhausting volumetric threats and blended application-level attacks, makes ADCs and load balancers a limited and partial solution for customers requiring best-of-breed DDoS protection.

Content delivery networks (CDN)

The truth is, a CDN can address the symptoms of a DDoS attack by simply absorbing these large volumes of data. It lets all the information in and through. All are welcome.

There are three caveats here. The first is that there must be bandwidth available to absorb this high-volume traffic, and some of these volumetric-based attacks are exceeding 300 Gbps, and there is a price for all the capacity capability. Second, there are ways around the CDN. Not every webpage or asset will utilise the CDN. Third, a CDN cannot protect from an application-based attack. So let the CDN do what it was intended to.

What is Arbor’s approach to DDoS protection?

“The fact that DDoS attacks have increased in size and the massive threat of bandwidth saturation should be of concern to all African organisations and organisations operating in the region as this region has not been immune to DDoS threats but has witnessed a steep increase in attacks. We are fortunately seeing an increased interest in DDoS detection and mitigation services in the territory,” says Hamman.

Arbor strongly believes that the best way to protect your resources from modern DDoS attacks is through a multi-layer deployment of purpose-built DDoS mitigation solutions.

“You need protection in the cloud to stop today’s high volume attacks, which are exceeding 300Gb/sec. You also need on-premise protection against stealthy application-layer attacks, and attacks against existing stateful infrastructure devices, such as firewall, IPS and ADCs,” adds Hamman.

“Only with a tightly integrated, multi-layer defence can you adequately protect your organisation from the full spectrum of DDoS attacks.”