How **DDoS Mitigation** is about **Corporate Social Responsibility**

We see the Network, we monitor the Network and we can protect your business with automatic DDoS mitigation services from our Network core. Regardless of what internet facing security you may already have, we understand your specific Network traffic profile and defeat DDoS attacks before they reach your defences.

Distributed Denial of Service (DDoS) attacks are on the increase by over 100% year on year

Be aware and prepared in the anticipation of a Cyber Security attack

Introduction

Distributed Denial of Service (DDoS) attacks have been impacting businesses across the world for many years now, and their effectiveness to cause damage to organisations has been well proven. In 2016 there was a huge upsurge in the use of DDoS attacks to cause mayhem and panic, proving the fragility of our belief that we had gone beyond this type of security threat.

DDoS does not appear to be going away anytime soon, which is why it is imperative that corporate organisations look to ensure that DDoS Mitigation is part of their Corporate Social Responsibility.

Contents

Integrated and Managed DDoS Protection within your Network

Threats are Constant and Increasingly Sophisticated

With a growth this year of 100% in DDoS attacks it looks like DDoS is not only here to stay but also in growth mode. What is interesting is that the types of DDoS attack have not changed but what has changed is the type of device that is making these attacks.

> ***"DDoS attacks have increased by over 100% year on year."***

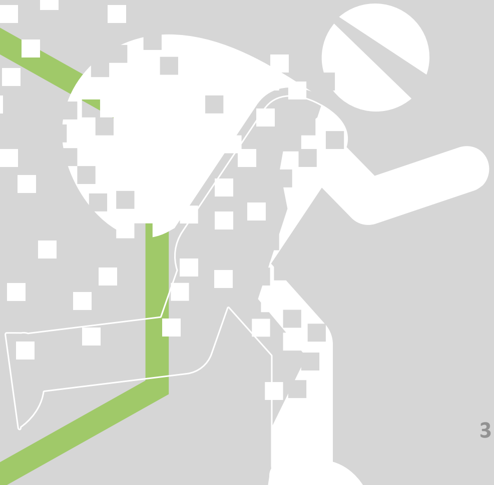
Historically it was the command and control server communicating with a botnet, composed of compromised computers, under which DDoS attacks were initiated. The compromised machine, turned into a zombie when joining the botnet, made the attack. But recent attacks have been performed using high volumes of native internet devices. In an attack in September 2016 the payload reached 1Tbps at the height of the attack, the whole attack is attributed to IP CCTV cameras in their thousands. These cameras are the forefathers of what we now describe as the Internet of Things (IoT).

Internet-connected devices provide another attack vector

The whole concept of the Internet of Things (IoT) is to enable and enhance our world with devices native and enabled for the internet that provide everyday services. In suppliers rush to bring these devices to market they have provided threat actors with the perfect platform for attack and potential extortion. In their haste suppliers have missed a key requirement when doing anything on the internet and that is security!

These devices are able to be compromised and controlled to bring attacks on any target without danger of retribution or identification. Calls from authorities in the US to "attack back" will do little in this scenario and certainly not restrict an attack as just more IoT devices can be recruited. These IoT devices are quite dumb and unable to register when they have been compromised or note differences to their environment.

Hackers can attack **any target** without danger of identification.



> *“There will be over 20 billion IoT devices by 2020.”*
>
> **Gartner**

> *“Investment in securing IoT devices will increase five fold over the next five years as adoption of these devices picks up.”*
>
> **Business Insider**

All this means that not only do IoT vendors need to deeply consider how they protect their machines but that there is already a considerable botnet army in place that it is available and easy to mobilise. Another interesting facet to this is that the availability of botnet DDoS attack vendors on the Darknet has increased significantly.

> *“Traditional IT security practices like network monitoring and segmentation will become even more critical as businesses and governments deploy IoT devices.”*
>
> **Business Insider**

Serious Cyber Security Threats for Corporates

For corporate organisations this manifests itself as an additional vector for consideration when protecting the IT estate. In recent years many businesses had taken to using their Firewalls or DDoS endpoint devices as being the way of looking at mitigating DDoS attacks.

On the face of it this seems like excellent economic sense. However, with attacks reaching such high volumes it becomes obvious that these types of devices would be very quickly inundated and the attack would become successful. No matter how clever an enterprise’s cyber security device is, the sheer volume of these attacks prove that threats need to be mitigated elsewhere.

With IoT vendors not even aware of the situation they have created it would be difficult to envisage that stopping the initiation of the attack will happen any time soon.

Corporate organisations also typically look at these types of attacks as being initiated from outside of their environment, but with these new exploitable IoT devices that may no longer be the case.

Corporate Social Responsibility (CSR)

So, how do corporate organisations avoid becoming the victim of a DDoS attack and stop devices within their estate from being exploited?

The first thing is to realise that DDoS attacks are often a way to disguise activities looking for other weaknesses that can be exploited. Very often devices such as IP CCTV cameras are less than protected unlike the corporate core.

The second thing is that corporate organisations need to realise that no matter how much money they have invested in the security devices that live in their data centres and on-site, the potential volume of these DDoS attacks dwarfs any capability they believe they may have at the delivery point of the attack.

Ultimately they are vulnerable to being taken offline, which will damage their reputation and have additional financial implications.

In a recent survey by Tech Pro Research, 69% of tech leaders said they'll be focusing on improving security for IT systems in 2017.

http://www.techrepublic.com/article/infographic-2017-it-budgets-are-increasing-and-spending-priorities-are-on-security/

From a Corporate Social Responsibility perspective it is in all corporate organisation's interest to ensure that they do not allow their devices to become tomorrow's botnet DDoS attack and that they protect other their services and the customer information they have from any risk.

The enterprise should ensure that compliance and monitoring plays an active role in regulating cyber security to protect critical information. Security and data privacy measures are necessary requirements to strengthen reputation with consumers. A robust strategy including services such as advanced DDoS Mitigation is essential to providing true value to users and stakeholders.

Exponential-e believe that the only true way to effectively protect a corporate from a DDoS attack is to mitigate the attack at the core of the network

Exponential-e's Approach

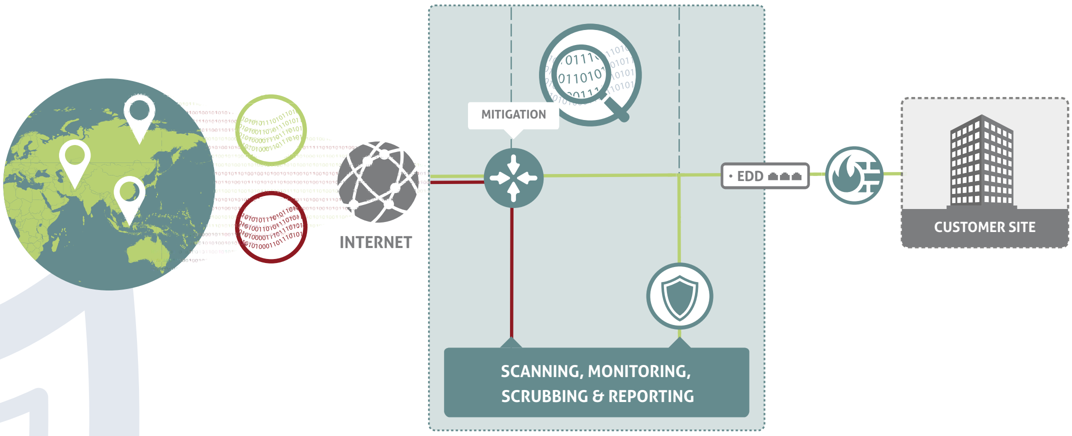
Exponential-e believe that the only true way to effectively protect a corporate from a DDoS attack is to mitigate the attack at the core of the network and therefore before the threat traffic can come anywhere near the corporate network and devices.

Exponential-e's Primary DDoS Mitigation service provides our customers with protection on the internet by diverting threat traffic automatically when our network sensors first see it, meaning we are able to provide an effective response to any DDoS attack. Our service offers the ability to focus particularly on the key elements of the corporate enterprise that are critical to performance and profitability.

This means we can also protect the corporate assets that may be targeted by an attack.

The Exponential-e Primary DDoS Mitigation service does not require any additional equipment and is provided to our corporate customers in conjunction with their internet services. This means that the investment already made in the protection of the corporate estate is not wasted, but supported by our service.

By using this service, corporate organisations are assured that they will save themselves from potential web outage if they were to be attacked, protect themselves from potential compromise concealed within a DDoS attack and maintain an expected level of Corporate Social Responsibility in the way they manage their Cyber Security.



exponential-e
APPLIED INNOVATION

www.exponential-e.com

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com