ELECTRIC™ LIGHTWAVE

# DDoS MITIGATION BEST PRACTICES

## DDoS ATTACKS ARE INCREASING EXPONENTIALLY

Organizations are becoming increasingly aware of the threat that Distributed Denial of Service (DDoS) attacks can pose. According to Arbors Network's 10th Annual Worldwide Infrastructure Security Report, organizations of all types and sizes faced disruptive DDoS threats to their business during 2014. Nearly half of all enterprises in the report were hit with DDoS attacks during the survey period, with almost 40 percent of those seeing their Internet connectivity saturated. With DDoS attacks becoming the number one operational threat to businesses, now is the time to become familiar with DDoS Attacks and what you can do to prevent them.

**42%**

**of companies surveyed this year reported more than 21 attacks per month.**

**Compared to 25% in 2013.**

*Source: Arbor Network's 10th Annual Worldwide Infrastructure Security Report*

### What are DDoS Attacks?

A DDoS attack is simply an attempt by an attacker to exhaust the resources available to a network, application or service so that genuine users cannot gain access. The majority of attacks that we see today are what we call Distributed DoS (DDoS) attacks—these are just DoS attacks launched from multiple different hosts simultaneously; and, in the case of a botnet, we could be talking about 10s, 100s or even 1,000s of machines.

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. 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. 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. TARGET SOME ASPECT OF AN APPLICATION OR SERVICE AT LAYER 7. These are the most critical type of attack 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 become prevalent over the past three or four years. Simple application layer flood attacks (HTTP GET flood etc.) have been one of the most common DDoS attacks identified.

Within these categories the actual attack vectors being used are evolving continuously. There has been a dramatic acceleration of innovation on the part of the hacker community. Hackers are coming up with new and more complex attack tools on a regular basis and it appears that no one is safe from attack.

**The DDoS landscape continues to change considerably and organizations are unprepared to deal with today's threats as highlighted by the number and severity of DDoS attacks reported in 2014.**

# WHY ARE DDoS ATTACKS PERVASIVE?

Over the past year we have seen the types and sizes of organizations being targeted broaden substantially. It's not just financial institutions and gaming sites being targeted, recently we've seen government departments hit, e-commerce sites and even pizza delivery companies targeted. Why this change? Well, here are a few reasons:

- **Easy to launch** – Anyone can download and launch an attack. The availability and awareness of attack tools have made DDoS attacks accessible to any person, organization or state looking for a way to impact another Internet user. Also, we should not assume that attacks generated by individuals will only be effective against another individual; some of the attack vectors incorporated in the readily available attack tools are stealthy and complex, and are effective against commercial systems with just a single attack source—if these systems are not configured or protected appropriately. More of a concern though is what happens when many people download the same tool and direct it towards a common target. In this case we effectively have a 'volunteer' botnet and more significant volumes of traffic can be generated, impacting larger and better protected targets.
- **Inexpensive to outsource** – It's easy to hire a botnet to carry out a DDoS campaign on your behalf. Numerous sites offer this 'service' and the rates are very reasonable—$5 per hour, $40 per day. This has led to the use of DDoS attacks as a competitive 'weapon' between rival businesses.
- **Devastating to business** – Some attacks are still motivated by extortion, blackmail and business competition while others want to purely gain an advantage in a virtual gaming world, but recently ideological hacktvism and Internet vandalism have come to the forefront as motivations. According to a 2011 Arbor Network's Worldwide Infrastructure Security Report, ideological hacktivism and Internet vandalism were voted the number one and two motivations behind attacks monitored by network operators responding to the survey.

A botnet can carry out a devastating DDoS attack for as little as **$40 per day**

## HOW TO REDUCE OR MINIMIZE ATTACKS

What should you do to protect your business from the DDoS threat? There are a number of things that you can do to reduce your threat surface and minimize the impact of any attack that include:

- **Understand the types and volumes of traffic on your network** – Know where traffic comes in, where it goes out, what it is etc., and understand your typical traffic for a given time of day and day of week. With this level of traffic visibility at layers 3, 4 and 7 you can proactively identify changes from the norm and recognize an attack or reconnaissance activity prior to an attack. If you know something is happening, or about to happen you can alter your security posture appropriately.
- **Establish a contact list before you're compromised** – If you are under attack, or feel an attack is imminent, knowing who to call is very important (but often overlooked). It is imperative that we know 'who' within our organizations, our service providers and our managed security partners is there to help us and 'how' we should contact them. If you don't have this information at hand, or the information is outdated, your ability to respond has already been compromised.
- **Develop an incident handling process** – Insist on a documented process for interactions with any managed security service partners. Having an incident handling process provides an important structure for dealing with an incident, when stress levels can be high. These processes allow incidents to be dealt with more quickly and can prevent people from taking 'risks' with security to try and solve an immediate problem (DDoS has been commonly used as a smoke screen for data exfiltration).
- **Practice and test attack scenarios** – Ensure your staff practices the incident handling process. Make sure all of the tools for defending against an attack are at your disposal and operating effectively and efficiently. Just having an incident handling process isn't enough—it must be regularly tested and proven to work.

> **"DDoS attacks have become a standard component of larger campaigns, often serving as a distraction or smoke screen for other malicious activity."**
>
> **Gary Sockrider,**
> Solutions Architect at Arbor Networks

## HOW TO REDUCE OR MINIMIZE ATTACKS

- **Block access effectively** – If you operate online services, restrict access to only the protocols and ports which are required. If you have a large number of repeat users or important customers, develop a whitelist of their IP addresses so that their traffic can be passed during an attack even if everything else must be dropped. Getting visibility of the traffic on your network will help identify the ports, protocols and repeat users for restricting access.
- **Use your infrastructure wisely** – If you need to restrict access to an on-line service or block attack traffic should you use your firewalls? You can, but many routers and switches support stateless Access Control Lists, implemented in hardware. This makes them ideal for controlling the traffic reaching your servers enforcing a white-list. And, can even be used to drop the traffic from sources identified as sending attack traffic. Dropping traffic here, rather than on any stateful firewall reduces your threat surface. Firewalls can exhaust their state tables and some attacks exploit this—routers and switches do not have this issue.
- **Leverage your relationships with your service providers** – Blocking traffic before it reaches your network perimeter protects your upstream links from becoming saturated during an attack. Some service providers have automated processes whereby customers can have traffic to/from particular sources blocked in this way.

All of these best practices can help you minimize the impact of DDoS attacks but they only provide partial protection from the threat. Your online services are vital to your company and DDoS attacks can render these services inaccessible to your customers, damaging your reputation and resulting in devastating losses to your business. To effectively defend against DDoS attacks you need to focus on mitigating DDoS attacks. There are generally two approaches for an organization to defend against DDoS attacks: deploy defense with your internal resources (a DIY defense) or use a cloud-based service. A DIY defense allows you more control with your IT team bearing the responsibility. This approach requires your organization to invest in tools and technical expertise. Many organizations already struggling with tight IT budgets and staffing opt to leverage the services of a cloud-based DDoS service.

### Key IT Challenges

Staffing issues resulting in a lack of technical expertise and operational experience to respond to DDoS attacks.

Communication issues during the critical stages of a DDoS attack between business leaders and IT often hamper effective defense.

Defense against DDoS attacks relies primarily on existing security services that are less effective than a focused DDoS mitigation service.

Planning and testing for DDoS attacks are inadequate and result in confusion and prolong the damage of an attack.

## SELECT AN EFFECTIVE DDoS DEFENSE

DDoS attacks are becoming more sophisticated and continually evolving in intensity, scale and scope. Companies of all sizes are having difficulties keeping up with the changing DDoS landscape and many are leveraging cloud-based DDoS mitigation services as an affordable solution that doesn't require capital investments. Additional benefits of a cloud-based DDoS mitigation service include the following:

- **Upstream location** – With defense upstream traffic in an attack is blocked before it can saturate your organization's connection. This minimizes impact to your company's Internet bandwidth and allows legitimate traffic and your business to continue.
- **Visibility** – Leveraging a service provider and their tools for analyzing your network traffic makes it easier to assess your network traffic and establish a baseline to accurately differentiate between normal and malicious traffic.
- **Management** – By using a cloud-based mitigation service, your organization gains access to a robust 24 x7 security operation team with the latest tactics to defend against evolving DDoS exploits.
- **Availability and Scalability** – Your organization gains the availability, infrastructure, network services and backup strategies of your DDoS mitigation service provider.

In a paper evaluating DIY and cloud-based service, Nemertes Research recommended-cloud base defense due to the unique nature of DDoS and the significant differences between the two options.[1] Relying on a cloud-based service enables your organization to cost effectively protect your online services with industry experts in DDoS attack mitigation while allowing your IT resources to focus on more strategic aspects of your business.

Keeping your organization secure requires a comprehensive plan that includes defense against DDoS attacks. Evaluate and update your comprehensive cyber security plan regularly and be sure you deploy the best solutions to protect your organization.

**CONTACT US**

**(877) 953-7747**

### ABOUT ELECTRIC LIGHTWAVE™

Electric Lightwave™, an Integra company, serves as a trusted network infrastructure partner to enterprises, government agencies and carriers in select markets throughout the western United States. We combine dense metro and intercity fiber assets, enterprise-grade network solutions, including Ethernet, Wavelengths and IP, with a highly responsive and easy to do business with approach. Electric Lightwave offers a premium service experience to match our premium network infrastructure solutions.

**VISIT US AT:**
electriclightwave.com

[1] http://www.business.att.com/content/whitepaper/Nemertes-DN2400-ATT-DDos-Issue-Paper.pdf