

# Protect Yourself from DDoS Attacks

Our top 10 anti-DDoS recommendations  
from our experience managing  
80,000 servers for over 10 years

# CONTENTS

<b>Introduction</b>	<b>3</b>
<b>Cybercrime 101</b>	<b>4</b>
What is a distributed denial of service (DDoS) attack?	4
Why do DDoS Attacks occur?	4
Top 10 industries attacked in 2015	5
DDoS Attacks are Getting Easier	5
The Impact of DDoS Attacks	5
Types of DDoS Attacks	6
DDoS Attacks During Times of Peak Traffic	7
<b>LeaseWeb's 10 recommendations for securing your environment</b>	<b>8</b>
<b>CONCLUSION</b>	<b>11</b>

# INTRODUCTION

A look at the headlines will tell you that distributed denial of service (DDoS) attacks have become a part of having a presence on the web. While the question used to be if you will be attacked, today it is only a matter of when. Government organizations, e-commerce, media and more have all been targets of DDoS attacks. Because of this, it is more important than ever to have a defense strategy in place. Preparation and planning will help you and your employees handle an attack when it occurs and can help to mitigate the impact on your reputation and financial bottom line.

In this white paper we will discuss in detail the current trends in DDoS attacks and their impact, as well as the different types of attacks, when they happen, and what you can do to protect yourself. We'll also cover some best practices, and how to work with a partner to help you set up the best possible defense for your site.

# CYBERCRIME 101

## WHAT IS A DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK?

A DDoS attack is an attempt from multiple attack sources to prevent legitimate users from accessing a machine or network connected to the internet. This is done by flooding the target system with large volumes of requests from multiple sources in order to either temporarily or indefinitely interrupt service. Because DDoS attacks make needed resources unavailable, they can have a significant impact on revenue, negatively affect user experience, and damage a business' reputation.

## WHY DO DDOS ATTACKS OCCUR?

According to the 2016 Verizon data breach incident report (DBIR), DDoS and web app attacks increased substantially from 2015. Successful data breaches of web app attacks where data was stolen increased from 7% to 40% with targeted data including:

- Credit card data
- Personal information
- Financial credentials
- Passwords

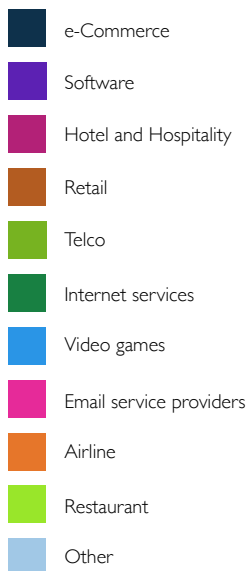
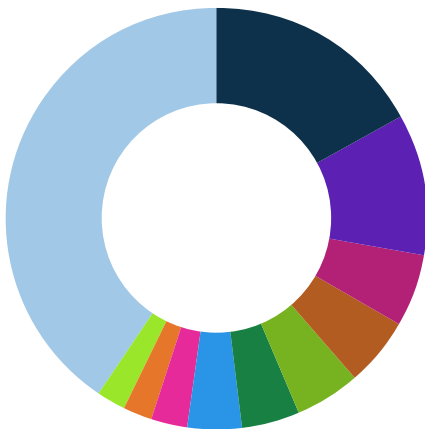
A majority of these breaches were discovered long after they took place by the credit card company or merchant bank.

The top targets for attackers are e-commerce, software, and hotel and hospitality. The focus on these industries makes sense because the data is likely to net the highest profits. E-commerce sites not only have large customer databases, they are often times associated with credit card numbers. This information can be quite lucrative for attackers.



## TOP 10 INDUSTRIES ATTACKED IN 2015

(SOURCE: HACKMAGEDDON)



The four main reasons behind attacks are: cyber crime, hacktivism, cyber espionage, and cyber warfare. Cyber criminals are responsible for over 70% of attacks with the motivation being either to steal company data or threaten to destroy it or prevent access to it until a ransom is paid. Hacktivists are usually motivated by political and social causes and use DDoS attacks to express their dissatisfaction with government, politicians, or business practices; one well known example is the group that goes by the name Anonymous.

Cyber espionage occurs when government or rival companies infiltrate competitor networks to steal confidential information. Cyber warfare involves one or more nation-states attacking another in order to disrupt or damage the target's network or, for example, to influence political outcomes by leaking confidential information.

DDoS attacks fall into three main types:

- Volume based
- Protocol attacks
- Application layer attacks

Attackers use one or more of these types of attacks for reasons ranging from simply slowing the performance of a site, to shutting it down completely, to stealing data or preventing access to it for extortion purposes. DDoS for ransom, or simply the threat of DDoS for ransom, is on the rise. In the latter, ransom notes are sent in the hope that threat of an attack will motivate a company to pay in order to avoid being a target. Bitcoin has become the standard form of currency for these transactions with the demand being anything from a few to hundreds of Bitcoins to prevent the attack. Armada Collective, Lizard Squad, RedDoor and ezBTC are some of the DDoS for ransom groups that came to prominence in 2016.

## DDOS ATTACKS ARE GETTING EASIER

It is easier than ever to launch DDoS attacks due to widely available automated tools that require no skills or special knowledge to use. There are also DDoS services for hire where a target can be anonymously attacked for only a few dollars. The sites offering these services sometimes call them 'stressers' to give the impression that they can be used to stress test your site, however they frequently do not verify whether you are the owner of the site or servers you are targeting. One such site, vDOS, offered its services to anyone with Paypal or a credit card. Tens of thousands of customers used the site to launch thousands of attacks.

The largest DDoS attack to date of almost 1 Tbps took place in September 2016 against OVH, a French global hosting provider. Almost 150,000 hacked Internet of Thing (IoT) devices, the majority of which were IP security cameras, were used to create a powerful botnet from which to launch the attack. With the growing number of unsecured devices such as appliances like smart refrigerators, remote home thermostat systems, and DVRs connected to the internet the likelihood of them being compromised and used in even larger attacks is greater than ever.

## THE IMPACT OF DDOS ATTACKS

What is the impact of a DDoS attack? During an attack the victim can lose customers if the site becomes too slow or completely inaccessible. If the attack becomes large enough the target's IP may be blackholed by the internet service provider in order to

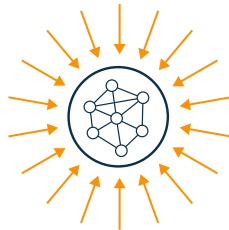
It is easier than ever to launch DDoS attacks due to widely available automated tools that require no skills or special knowledge to use.

mitigate the damage to the ISP's other customers. Depending on your agreement and configuration with your ISP, it could be days before your IP is allowed to accept traffic again and you may be required to pay for the extra load that was on the network .

On average it costs about \$50,000 per attack for smaller organizations and almost half a million on average for larger enterprises. However, the impact of an attack is not limited to the dollar amount from lost business. Employees will be need to work extra hours or move focus from other projects in order to locate the source of the security issue and develop a plan to patch, update, or upgrade hardware and software as needed. The reputation of a business can suffer not only because customers may become frustrated with slow loading or timeouts, but also if their personal or financial data is stolen. Such incidents can cause a company to incur legal expenses, higher insurance premiums, lower credit ratings, and the loss of future business.

## TYPES OF DDOS ATTACKS

As mentioned earlier, there are three main types of DDoS attacks: volume, protocol, and application. Let's look at each of these types in depth:

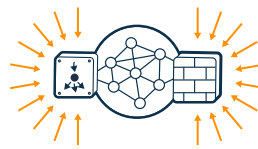


### VOLUME BASED ATTACK

A volume based attack relies on swarms of requests, usually from illegitimate IP addresses, to overwhelm a website with a flood of traffic. The intent of these attacks is to use up available bandwidth in order to prevent legitimate traffic from accessing the site.

**Common attacks:** UDP and ICMP floods

**Measured in:** bits-per-second (bps)

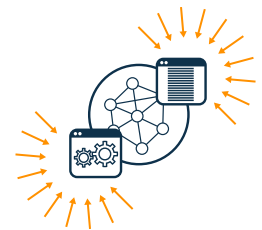


### PROTOCOL ATTACK

The goal of protocol attacks is to drain system resources by sending open requests such as a TCP/IP request with phony IPs, saturating network resources to the point that those resources can't respond to legitimate requests.

**Common attacks:** Smurf DDos, Ping of Death, and SYN floods. Another type of protocol attack includes sending large fragmented packets to overwhelm the system.

**Measured in:** packets-per-second (pps)



### APPLICATION LAYER ATTACKS

Layer 7 attacks are slow and stealthy by sending seemingly harmless requests that appear to be normal human interaction meant to bring down a web server or steal data. These attacks commonly target HTTP using a botnet.

**Common attacks:** Slowloris, Apache Killer and Cross-site scripting, SQL injection, and Remote file injection.

**Measured in:** requests-per-second (rps)

DDoS attacks are increasing year over year at about 50% annually. Layer 3/4 attacks are growing in size from 20 gigabytes per second up to several hundreds of Gbps . While volume and protocol attacks can be disruptive enough on their own, it is becoming more common for attackers to combine them with layer 7 application attacks in order to distract the target while their systems are breached and data is altered or stolen. These are called multi-vector attacks and are extremely effective.

## DDOS ATTACKS DURING TIMES OF PEAK TRAFFIC

Black Friday and the holiday season often generate over 30% more sales for online retailers which makes the last two months of the year a prime time for DDoS attacks. Large volumes of traffic and customer data, both personal and financial, make attractive targets for criminals during November and December. A well-known breach happened to the American retailer Target in December 2013 when attackers waited until the end of the holidays to pillage about 40 million customer credit and debit records. The fallout from this event resulted in the loss of customer trust, a drop in sales, a decrease in employee morale, and eventually the resignation of the CEO after a \$39 million lawsuit settlement with several U.S. banks that had been forced to reimburse customers who had lost money due to their credit card numbers being stolen.

## LEASEWEB'S 10 RECOMMENDATIONS FOR SECURING YOUR ENVIRONMENT

Now that we have a sense of the prevalence, scope, and types of DDoS attacks, the question becomes what steps you can take to prevent or mitigate them. The first thing to keep in mind is that security cannot be an afterthought - something to take into consideration once you've already configured your network, built out your servers, or written your software and pushed it to production. With every upgrade, code update, or new project, the discussion should also include what measures should be taken to ensure that the changes do not make your systems and resources vulnerable to attack. The following checklist can help you keep track of security concerns throughout your planning process:

- 1 Code with security in mind** - identify your security requirements before you start writing code. Have a set of security coding standards and ensure that developers are following them. Vigorously test your code to prevent some of the common types of vulnerability exploits such as cross-site scripting and SQL injection.
- 2 Develop emergency plans for patching and rolling back code** - have a detailed plan in place when pushing out new code so that if an issue arises it can be rolled back with little impact to your environment. This might include having a list of the developers on-call for each department, a central chat or war room to discuss the issue and what needs to be done, documentation, etc.
- 3 Keep patches up to date** - be aware of the latest patches available for your software and have a plan in place to both implement them and to roll them back if issues arise after the update.
- 4 Limit access to your environment** - ensure admin and/or root accounts are secure and that passwords are changed on a regular basis. Audit your access list frequently and be sure to remove access for any employees that have left



You can gain capacity and speed up site performance by utilizing Content Delivery Networks which also act like a barrier between origin server and the end-users.

the company. It is also important to change root and admin passwords if an employee who has left had access to those as well. Do not store passwords in plain text or collaborative documents.

**5 Do not expose admin interfaces to external networks** - admin interfaces should only be accessible from internal networks either via direct connection from that network or through a VPN. Test and verify that no one on an external network can access these interfaces. Be sure to remove VPN access for employees who have left the company.

**6 Add DDoS attack into your disaster recovery/business resumption plans** - disaster recovery should not just cover natural disasters such as storms, floods, or fires but also for attacks on your network and data. Your plan should include what to do and who to contact when you discover you are the target of an attack. Items to consider might be: how do we detect and verify that we are under attack? Do we have an emergency contact list of partners such as ISP or cloud providers? What is the escalation tree for each department? Who is responsible for talking the the media?

**7 Vulnerability scanning** - run a vulnerability scan to detect issues within your infrastructure and and code base so that you can mitigate your risk. A simple OWASP Top 10 Vulnerability test can reveal most crucial vulnerabilities. It is also good to run penetration tests on your network to detect any weaknesses that can be exploited.

**8 DDoS mitigation: Always on or On-Demand** - DDoS mitigation HW providers can be very expensive. If you don't have room in your budget to always be behind one, you still have the opportunity to move behind an On-Demand mitigation service. An On-Demand solution allows you to have the service contracted and effectively turned off until you are attacked. If an attack occurs, your traffic is routed to the mitigation service with a simple traffic routing change. The difference can mean a few of minutes of downtime versus a much longer period.

On average, if you haven't already subscribed to such service, it takes 24 hours to move behind a DDoS mitigation provider in emergency and can take up to 5 days to tune the environment so that all aspects of your site are rendering correctly. It is important if you are using a pre-staged service to ensure that the activation time of your supplier is limited to only 1 or 2 minutes so that the impact of an attack is limited.

**9 Leverage a CDN partner** - You can gain capacity and speed up site performance by utilizing Content Delivery Networks or CDNs. A CDN is a service that delivers webpages and other Web content through a distributed network. It distributes high levels of traffic across multiple servers to ensure that users accessing the site do not experience lag based on their geographical location. So although the primary benefit of a CDN is speed, CDN acts as well like a barrier between origin server and the end-users. Be sure to have your CDN setup and tuned before you enter your peak period.

**10 Web Application Firewall** - Traditional firewalls decide if one device can talk to another at the network level but a Web Application Firewall (WAF) monitors behaviors between a web site or an application and browser and inspects the traffic to verify if the request is legitimate or malicious. By operating at the application level, it can detect attacks based on stored patterns as well as

monitor for unusual or unexpected patterns. Application layer attacks are increasingly common in e-commerce making WAFs an essential part of your environment.

Like a CDN, WAF services can be provided via globally distributed architecture in the cloud. It requires some expertise to ensure that the rule set is configured to respond properly to your application and traffic. Allow yourself enough time to test or lean on the expertise of your supplier and tune your WAF before your busy season. Tuning WAF after every major application release is also a good way to keep this element of your environment healthy.

## CONCLUSION

Each year we have the feeling that we have seen the largest cybersecurity threats taking place but only instants later we find out that such record is broken by a new one stealing more credentials, using a bigger botnet, reaching higher bandwidth peak or disturbing an even more visible event. A notable trend in DDOS is the widening field of victims across all industries. So ensure that your company is taking these recommendations seriously and has a plan in place because 2016 headlines were likely only setting the stage for a new wave of breaches for 2017.



**NL** +31 20 316 2880  
**US** +1 571 814 3777  
**DE** +49 69 2475 2860  
**SG** +65 3158 7350

**[www.leaseweb.com](http://www.leaseweb.com)**  
**[sales@leaseweb.com](mailto:sales@leaseweb.com)**