# A Timeline to a DDoS Attack

## Anyone Can Launch a DDoS Attack

Tools for carrying out a DDoS attack are easy to find and download from the Internet. A Botnet offering DDoS attack services is easy to hire and inexpensive–available for as little as $40 per day and more companies are being targeted for reasons that include extortion, blackmail, business competition, ideological hacktivism or just plain Internet vandalism. It's so easy, anyone can execute a DDoS attack and everyone is vulnerable. How you defend against an attack can impact the future of your business.

## What Happens During an Attack Without DDoS Mitigation

### Without DDoS Mitigation

You believe your on-premise firewall is adequate and your business is not a target for would-be attackers.

Your website receives malicious data and tries to respond. It begins to slow down.

Your bandwidth is quickly consumed by the flood of data, only a few data packets in a thousand are from real traffic.

Your website is overwhelmed and unable to keep up with the data. It goes down and is unavailable to legitimate traffic.

While your IT team is distracted by the DDoS attack, the attacker can steal your confidential data from unprotected paths and cause more damage to your business. A DDoS attack is often used as a disguise for data theft.

Your IT team is still working on damage control.

Your business has been disrupted; your brand reputation tarnished and you're busy totaling the losses and damages.

You're identifying the confidential data compromised and notifying impacted customers or partners.

You may have to deal with possible fines and lawsuits from the attack and government mandated security audits.

## Pre-DDoS Attack

One of the most frequently observed threats on enterprise networks are DDoS attacks.

## DDoS Attack Begins

A flood of malicious data reaches your website.

## DDoS Attack Intensifies

Malicious traffic from numerous sources targeted toward your website multiply exponentially.

## DDoS Attack Ends

The flood of malicious data subsides.

## 24 Hours Later

Your website is back online, the seige is over.

You decide the threat is too big to ignore and decide to invest in a DDoS Mitigation Service.

An analysis is performed on your network to establish normal traffic patterns and a defense perimeter is established around your network.

Your network traffic is actively monitored and comprehensive detection mechanisms are deployed to detect potentially malicious traffic.

You are alerted that there is an attack on your network; you call the Security Operations Center to start the mitigation process.

Traffic is rerouted to a scrubbing center and malicious traffic never reaches your premise.

Your network remains available and you continue business as usual while the DDoS attack is mitigated.

Your network is continually monitored and your network traffic is filtered; ensuring only legitimate traffic reaches your network until the attack subsides.

The Security Operations Center continues to monitor and ensure traffic is clear for 24 hours.

Traffic is rerouted back to its normal path.

All network traffic is normal and your company has survived a DDoS attack.

### With DDoS Mitigation Service

## What Happens During an Attack With DDoS Mitigation Service

## Is Your Business Prepared?

DDoS attacks like these occur every day and the only difference in the outcome is based on how you have prepared. It's time to consider your defense options for DDoS attack mitigation.

Electric Lightwave's DDoS Mitigation Service is part of Electric Lightwave's comprehensive cyber security suite designed to protect your business from a wide range of evolving online threats.

Learn More: electriclightwave.com

ELECTRIC LIGHTWAVE™