Common #DDoS Attack Myths

corero
FIRST LINE OF DEFENSE

1

MYTH: We are fully protected with cloud based DDoS mitigation.

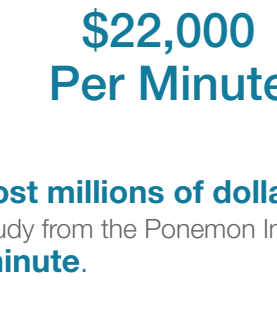
41% of attacks are **ONLY** Volumetric

FACT: Cloud based DDoS mitigation **only protects against large, volumetric attacks**, and fails to provide adequate protection against low and slow application layer attacks.

2

MYTH: DDoS attacks are only volumetric in nature.

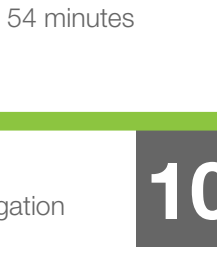
FACT: The reality is that DDoS attacks come in all shapes and sizes. The most damaging DDoS attacks, which mix brute force (volumetric) attacks with targeted, application-specific attacks, have much the same frequency at 39%, as targeted at 42% and volumetric at 41% alone.



3

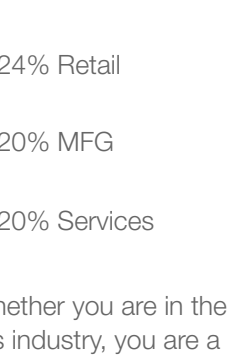
MYTH: We won't become a target. Our business is too small.

FACT: DDoS attacks don't discriminate. Any organization, **big or small, is in danger** of experiencing the risks associated with a DDoS attack.



4

MYTH: Our firewall can protect against DDoS attacks.



FACT: Firewalls can't protect against complex DDoS attacks, and instead, **act as DDoS entry points**. Attacks pass right through open firewall ports which are intended to allow access to legitimate users.

5

MYTH: My ISP is protecting me from DDoS attacks.

FACT: **ISP's lack the ability to detect, analyze and mitigate DDoS attacks** and other cyber threats before they can have a detrimental impact on the services they have contracted to deliver to their customers.

6

MYTH: My web properties are managed by a hosting provider, I don't have to worry about DDoS.

FACT:

Sheer volume of customers within a hosting environment **increases attack surface, and innocent bystanders** can easily become collateral damage when an attack occurs.

7

MYTH: Single configuration DDoS protection will provide adequate protection.

FACT: Not true. You need to make sure that your DDoS defense system can:

- Provide **granular DDoS configurations** (policies)
- **Defend** against all known **DDoS attack** vectors
- **Handle** the **load** while **under** a DDoS **attack**
- **Cannot be DDoS'ed** itself as part of a DDoS attack
- Provide access to **24X7 DDoS** defense **Support Services**

8

MYTH: DDoS solutions aren't worth the investment.

Average Attack Time:		Average Cost:		Average Total Cost:
54 Minutes	x	$22,000 Per Minute	=	$1,188,000.00 Cost per Attack

FACT: A DDoS attack **can cost millions of dollars** in lost business, brand damage, threat exposure and customer attrition. According to a study from the Ponemon Institute, average downtime due to DDoS attacks is 54 minutes with an average cost of **$22,000/minute**.

9

MYTH: My industry isn't a target for DDoS attacks.

FACT: Industry doesn't matter. Whether you are in the financial, retail, manufacturing or services industry, you are a target for DDoS attacks.

10

MYTH: We need a different DDoS mitigation tool for each type of DDoS attack.

FACT: Certain DDoS defense systems can provide protection for all different types of DDoS attacks. It's just a matter of finding the right one.

Source: Verizon 2013 Data Breach Investigations Report, Fortinet Blog: Myths about DDoS, Ponemon Institute, SANS DDoS Attacks Advancing and Enduring: A SANS Survey

corero
FIRST LINE OF DEFENSE

1 Cabot Road • Hudson, MA 01749 USA • Phone: 1.978.212.1500 • www.corero.com