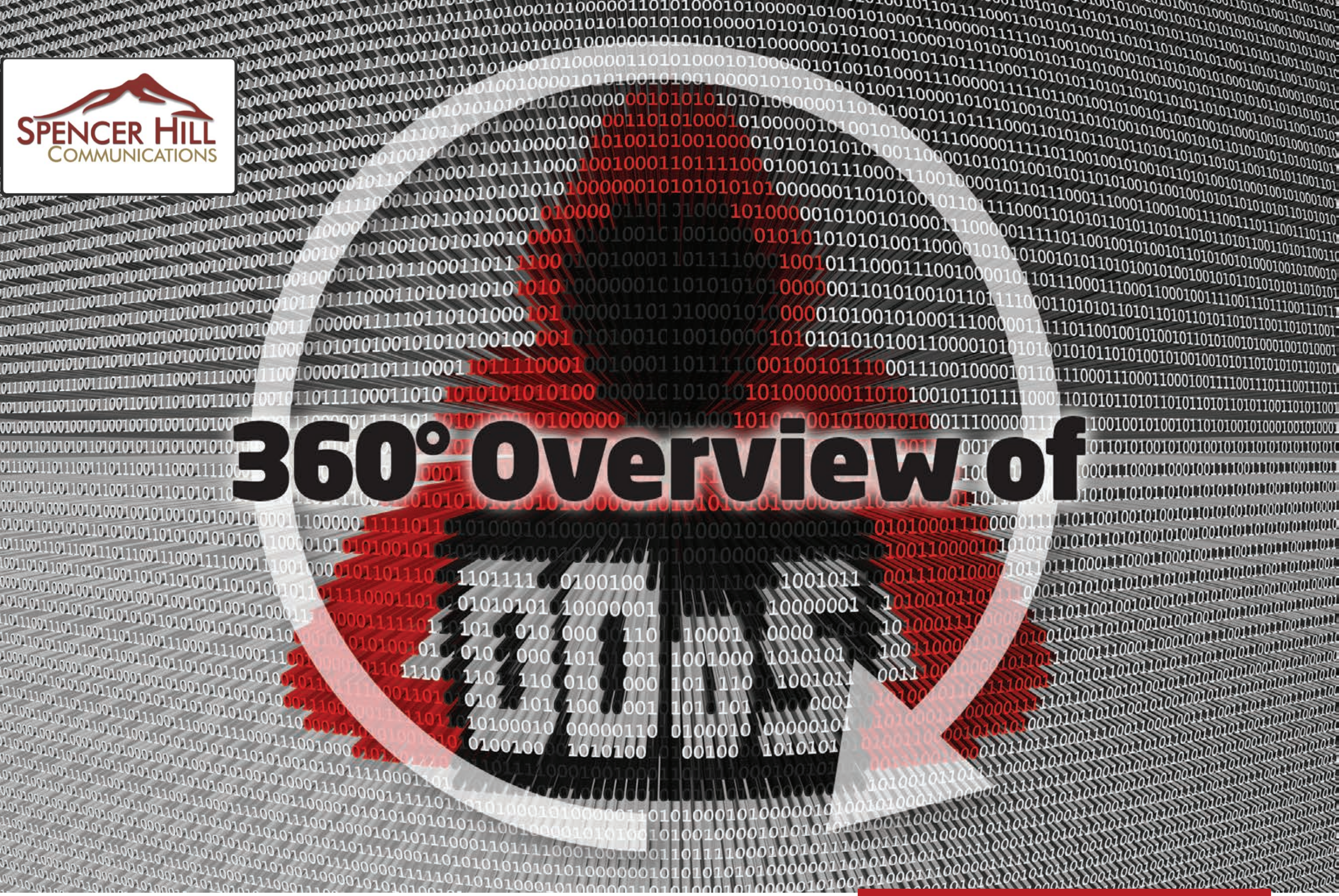
Spencer Hill
Communications



360° Overview of DDoS

What is DDoS

Short for distributed denial of service, DDoS attacks occur when a massive influx of web traffic from a multitude of IP addresses floods a machine or network resource. The network overloads with bogus traffic, causing all systems to shut down and preventing legitimate requests from being fulfilled.

(Think of it as a group of protestors crowding the entrance of a store to block patrons from coming in.)

Frost and Sullivan DDoS Mitigation Global Market Analysis –

Market grew 449.5% in 2014 and is expected to grow to

$977.2 million by 2019.

What are its Implications?

Revenue Loss	Downtime can affect bottom line up to and over $300K/hour (Gartner)
Productivity Loss	Critical network systems become unusable, halting productivity of workforce
Reputation Damage	Customers lose trust because site is inaccessible and their data is stolen
Theft	Funds, customer data, and intellectual properties can all be stolen

Examples of Significant Attacks

BBC (December 31, 2015)
Considered the largest attack in history. Website was shut down for multiple hours.

Blizzard Entertainment (April 13, 2016 and August 23, 2016)
Development studio behind World of Warcraft. Hit by two attacks, both of which caused latency, connection, and login issues for its customers.

The US Library of Congress (July 18, 2016)
Multiple websites were inaccessible through a "massive and sophisticated DNS assault."

NSA (October 25, 2013)
This organization, dedicated entirely to "the protection of U.S. government communications and information systems," had its website shut down by a DDoS attack.

Can you afford to risk to your reputation or lose prospects and sales if your website goes down or your network is breached?

Statistics on DDoS

Longest DDoS attack in Q1 2016 lasted for **8 days**

- Kaspersky Lab

Frequency of DDoS attacks has **increased more than 2.5 times** over the last three years

- Cisco

DDoS attacks in Q4 2015 spiked **40%** from the previous quarter

- Akamai

Botnets amplify DDoS attacks and cause over **$113 billion** in losses globally each year

- FBI

A DDoS attack can be purchased for **as little as $5**

- Dell SecureWorks

Prevent Attacks with DDoS Mitigation

Identify the right network-based security protocols and solutions. DDoS mitigation techniques employed by best-in-class providers include:

- Re-routing internet connections and "traffic-scrubbing" filters
- Behavioral analytics and threat intelligence
- Application monitoring
- Real-time reporting

With the growing rate of attacks, it's recommended for all businesses with public-facing IP addresses or DNS servers to have anti-DDoS tech and an anti-DDoS emergency response in place.

Providers with DDoS Mitigation Solutions

CenturyLink®
Channel Alliance
Premier Elite Alliance Member

Level(3)®
COMMUNICATIONS
Connecting and Protecting the Networked World℠
ELITE
CHANNEL PARTNER

MASERGY

verizon✓
partner program - platinum

Discovery Questions

- What partnerships, technology and processes do you currently have in place to protect your environment?
- What third-party vendors do you work with that could potentially leave you vulnerable, allowing access to your network?
- What is the status of your emergency response plan (incident response plan)?
- Do you have a business continuity plan in place?
- What in-house expertise do you have to react to an incident that occurs?
- Are you aware of the implications a DDoS attack can have on your businesses?