DDoS

TBI Battlecard

What are the implications of a DDoS attack?

- 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 has been stolen
- Theft – Funds, customer data, and intellectual properties can all be stolen

What to Look for in the Field

- Customers with self-hosted applications or websites. This could include their inventory or logistics applications, or phones.
- Customers relying on internet for their business.
- Customers that have been attacked before.

Overview

Short for distributed denial of service, DDoS attacks are when a massive influx of web traffic from a multitude of IP addresses floods a machine or network resource. As a result, all systems shut down, preventing legitimate requests from being fulfilled. Think of it as a group of protesters crowding the entrance of a store to disrupt normal operations and keep buyers out; it's essentially the same thing.

DDoS mitigation protects attacked networks by passing internet traffic through "traffic scrubbing" filters. More specifically, it correctly identifies human traffic from bots and hijacked web browsers by examining attributes like IP address, cookie variations, http headers, and Javascript footprints. Because of how common DDoS attacks are these days, it's recommended for any business with public-facing IP addresses or DNS servers to have anti-DDoS technology and an anti-DDoS emergency response in place.

Discovery Questions

Security risks are more advanced and abundant than ever. Because of this, your clients are relying on a consultant to provide the solutions needed to keep their sensitive data protected and their systems clear of malicious bot activity.

Good questions to start the conversation with your customers:

- 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 by allowing access to your network?
- What is the status of your emergency response (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 business?
- Does your business reply on the internet, SaaS/Cloud applications?
- Can you withstand being offline? For a day or more?

Debunking Myths

- I'm too small to be a target
- We have never been attacked, so never will
- We were attacked by DDoS but it stopped
- If DDoS attacks were a problem, someone would have told me
- My cyber insurance will cover it
- DDoS attacks are not a big deal, downtime doesn't hurt my business
- DDoS attacks only affect websites and API endpoints
- I'm ok if I have enough bandwidth
- I have a good router

Add-ons to DDoS

Web application security

Ask about security as it relates to:

Cloud Infrastructure, Email and Web, Threat Management and Response

Top Providers

AT&T | CenturyLink | Level 3 | Masergy | Verizon