MAZEBOLT

CASE STUDY

Eliminating DDoS Mitigation False Positives

This global banking and financial services company is committed to providing reliable services and tools to its account holders. Setting up and using the company's services is ridiculously easy for customers, but behind this facade lies a complex, secure, and highly intelligent platform with intricate applications and networks working seamlessly. That is, until a single incident, spiraled into a complex DDoS mitigation reaction, resulting in legitimate customers being blocked.

The Challenge

The client was adding new services, to increase sales and customer engagement for their merchants. One of the applications inadvertently sent customers a push request that caused a flood of legitimate responses from them. Their DDoS mitigation solution mistakenly identified the legitimate requests as a DDoS attack and end-users were blocked.

Thousands of customers were denied access during this unfortunate event and damage control took a heavy toll on the company's resources and reputation. Going forward, they wanted to ensure that their DDoS mitigation solution could keep up with the dynamic pace of change introduced to their network environment by the digital transformation without causing false positives.

Customer snapshot

Description

A European multinational banking and financial services company with over 2000 employees serving millions of global customers, corporates, and financial institutions.

Industry

Financial Services

Business stats

The company has remained at the forefront of the digital payment revolution for over two decades. The next-gen technology-enriched online platform offers consumers and merchants in more than 200 markets the seamless opportunity to join and thrive in the global economy.

The Solution

MazeBolt's RADAR™ solution empowered the client to identify mitigation of legitimate requests automatically, continuously, and non-disruptively. RADAR™ working as an additional layer on top of their DDoS protection solution provides visibility on legitimate requests that are blocked towards each web-facing IP/target in their network environment.

The client's DDoS mitigation vendor uses the false-positive insight from RADAR™ to fine-tune their DDoS protection policies. By continuously validating their web-facing services against both legitimate traffic and malicious DDoS attacks two things happened:

- **False Positive –** RADAR™'s insight helps configure DDoS protection policies to ensure no legitimate traffic is being blocked.
- **DDoS Protection –** RADAR™ continuously identifies holes in their DDoS mitigation policies that allow attacks to penetrate before the attacks are launched, effectively eliminating DDoS risk.

The Benefits

The client's CISO has complete, continuous and most importantly proactive visibility into vulnerabilities that allows him to secure the integrity and online availability of their services, no matter what changes their digital transformation process requires – all with minimal resources.

RADAR™'s automatic and continuous operations provided quantifiable metrics that allow the security team to clearly monitor and reflect the risk status to management. At the same time, these metrics provide a common language to communicate the security implications of all network changes introduced to the respective teams across the organization.

And finally, RADAR™ ensures pre-emptive attack surface defense of the client's network without replacing existing DDoS mitigation. This allows security teams to focus on prioritized vulnerabilities saving valuable time.

About MazeBolt

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.

For more information,
please visit: www.mazebolt.com
or e-mail: info@mazebolt.com