MAZEBOLT

Case Study:
Insurance

Leading insurance company uses RADAR™ to eliminate the DDoS threat.

Overview:

For a leading North American insurance company catering to a customer base of over 4 million and boasting yearly revenues of over $12 billion - having 24/7 online availability is more than critical. Recently, the company has undergone a comprehensive digital overhaul, enhancing its offerings by delivering essential services and mobile applications to its valued customers, agents, and staff. Nevertheless, the organization's security teams struggled to prevent damaging downtime due to ongoing DDoS attacks.

The Challenge:

In recent years, the company experienced downtime due to DDoS attacks, despite having the best hybrid protection solutions in place that includes Scrubbing Center and on-premises DDoS protection. A rough estimate of DDoS downtime costs indicated a multi-million dollar loss, and online reputational damages. Bi-annual traditional DDoS tests were disruptive and inconvenient, required maintenance periods, and weren't effective in preventing attacks. In addition, they identified only a fraction of the vulnerabilities and lacked actionable remediation plan.

Recognizing the massive incline of DDoS attacks, the frustrated cybersecurity team was looking for ways to significantly reduce the risk and prevent damaging attacks.

And this is where MazeBolt RADAR™ came in.

The Insurance DDoS Threat

- Disruption to critical mobile and online services.
- Disruption to claims and payment processes.
- Agent productivity loss when agent portal is unavailable.
- Employee productivity loss when VPN and email servers are down.

THE SOLUTION:

After a short POC, it was clear that over 54% of Layer 7 attacks were not blocked and would certainly cause downtime. With continuous and non-disruptive testing, MazeBolt's innovative solution could easily expose all DDoS vulnerabilities, and therefore, the company decided to deploy RADAR in three data centers, downstream of each of their DDoS protection layers.

Fully deployed, RADAR uncovered the following:

> Over 2800 DDoS vulnerabilities > 63% of DDoS vulnerabilities across layers 3, 4, and 7 > Automated DDoS protection was only 37% effective > Emergency response teams and SLAs will not prevent DDoS downtime

MAZEBOLT

While conducting the first round of testing, RADAR identified that the company didn't have layer 7 DDoS protection and required SSL off-loading to enable it. The enormous volume of vulnerabilities left the company's environment unprotected. When the next DDoS attack hits, manual intervention of emergency response teams will be required, resulting in damaging SLA's TTM (time-to-mitigation).

RADAR automatically provided a prioritized remediation plan of all vulnerabilities, including Slowloris, UDP, IKE, and DNS attack vectors. MazeBolt's Professional Services team helped manage the remediation process, working side-by-side with the client's DDoS mitigation vendors' SOC teams.

THE BENEFITS:

RADAR delivered the following results:

- Over 93% of DDoS vulnerabilities in layers 3,4, and 7 were identified and eliminated, in less than 6 months.
- Automated DDoS protection was improved by over 150% A WAF solution was chosen and deployed based on
- RADAR's recommendation, to make sure Layer 7 attacks will be automatically blocked
- The DDoS vulnerability level has been kept in the low single-digits
- The need to initiate damaging TTM and emergency response SLAs was eliminated

Since deploying RADAR, and despite being heavily targeted by various threat actors, all DDoS attacks have been mitigated automatically without any damaging downtime. Ongoing RADAR validation provided the necessary insight and data to maintain and protect new services.

RADAR deployment is currently extended to the cloud. The new cloud deployment will be centrally managed with their existing on-premise deployment and create a unified vulnerability flow with their mitigation vendor.

They have now adopted the new approach to DDoS security with RADAR: Preventative, Proactive, automated Protection.

> Following our work with MazeBolt, I felt our previous DDoS protection efforts were a "placebo".
> MazeBolt provided us critical insights to remediate all of our DDoS risks.
> I'm confident our systems are much safer today with RADAR and our DDoS protection is as resilient as possible.

CISO,
a Leading Global Insurance Company

MazeBolt is pioneering a new standard in DDoS security. RADAR™, an industry-first patented solution, empowers organizations to identify and remediate vulnerabilities in every layer of DDoS protection. Global enterprises, including financial services, insurance, gaming, and high-security government environments, rely on MazeBolt to prevent damaging DDoS attacks.