Tailoring DDoS Test Simulation to Suit a Multinational Company's Architecture

RED BUTTON
DDoS Experts

BACKGROUND

A multinational company, specializing in digital automation and energy management, approached us to evaluate the efficiency and effectiveness of their existing infrastructure and protection measures against DDoS attacks.

The company uses Azure cloud services, including, Azure DDoS Protection. However, the company uses a specialized HTTPS-based protocol that utilizes mTLS certificate validation, and wanted to know whether an attacker would be able to exploit this to generate a DDoS attack.

THE SOLUTION

The Red Button team carefully analyzed the company's cloud architecture, we planned and executed multiple attack vectors, including volumetric, protocol, and application layer attacks, to stress and identify weak points in the existing protection.

THE RESULTS

Five of the six attack scenarios were fully mitigated by the Azure DDoS Protection service without impacting the company's services.

However, the application-level attack scenario was neither detected nor mitigated, and it caused an immediate downtime to one of the company's services. This deficiency could potentially pose a significant, costly threat to the global organization's business continuity.

RECOMMENDATIONS

To address the identified protection gaps, Red Button provided the following recommendations:

- **Improve Traffic Capacity**

  Our simulation revealed the system's inability to handle a relatively small amount of traffic. We advised modifying the hardware, software, and configuration of the service to support larger traffic volumes.

- **Configure Rate-Limit-Based Rules**

  To prevent users from submitting a large number of HTTPS requests, we recommended defining rate-limit rules in the WAF as an additional protection measure. Rules should be defined based on the typical expected behavior, with a threshold that is high enough to block malicious users and low enough to prevent false positives.

- **Apply Geo-Protection at the Network Layer**

  The existing protection solution settings exposed the company to network-layer attacks originating outside the location of its intended North American user-base. To limit this risk, we recommended tweaking the WAF settings to include geo-blocking, as well as setting geo-protection rules in Azure's network security groups to prevent layer 3-4 attacks.