Case Study

Industry Supply Chain Leader

AT&T Cybersecurity

DDoS attacks solved by Prolexic DDoS Cybersecurity Services

Solutions

- AT&T Content Delivery Network (ACDN) Prolexic Volumetric DDoS Service
- ACDN Edge DNS

Organization type

- Supply chain business (local and government)

Overview

A large supply chain company was subjected to a cyberattack and was mitigating the DDoS attacks internally using its own technical resources and an additional solution from a third-party provider. The AT&T account team, upon learning of the situation, presented their comprehensive portfolio of Cybersecurity solutions. This case study discusses how AT&T Cybersecurity implemented an always-on, carrier agnostic, volumetric DDoS solution to fortify the business's defense, thereby safeguarding it against future DDoS attacks.

Introduction

A large supply chain leader encountered a series of DDoS cyberattacks. To counter these, the firm deployed in-house mitigation strategies, involving manual intervention at the router and firewall levels. Their existing security consulting partner recommended adding an additional vendor as an extra layer of support. However, this approach resulted in the unintended blocking of valid clean traffic, adversely impacting the company's downstream business units. In response, the company initiated exploration of the volumetric DDoS market, which led them to AT&T. Upon understanding the gravity of the attack, AT&T presented our Cybersecurity portfolio, highlighting features such as a managed services platform, carrier agnostic approach, and an industry leading zero-second mitigation SLA. The firm, convinced of AT&T's competitive edge and value after several technical workshops, opted for AT&T's solution. Additionally, during the sales process, we were also able to sell upgrades to the customer's subsidiaries.

A key moment in the process was the series of workshops held between the customer and a large team of technical experts from AT&T. These workshops expedited the customer's understanding to quickly see the value of an always-on solution that also enabled the company to perform its own forensic investigation of each attack.

- **AT&T, in close collaboration with the customer** and the AT&T-sponsored technical team, tailored the solution to meet the company's specific needs.
- **AT&T successfully demonstrated to the customer** the power of the ACDN Prolexic DDoS always-on solution in combating volumetric DDoS attacks. Since the customer used multiple internet providers, a carrier agnostic solution was critical.
- **Edge DNS was integrated to protect the customer** from non-existent domain attacks and other potential threats to their DNS resolvers. This ensured that the company's end customers could sustain their access, regardless of any such attacks.

Challenges

- **The customer did not have an always-on DDoS** solution in place. This left them vulnerable and unable to quickly defend against a sustained DDoS cyberattack on their business systems.
- **The customer attempted to mitigate the attack** manually in-house with the help of DDoS mitigation tools supplied by a third party. However, this approach led to additional business impacts as valid clean traffic was being blocked along with the attack traffic.
- **The attack drained the company's technical resources**, which were needed to maintain the manual mitigation efforts.
- **The customer realized that they could not leave their mission-critical architecture at risk** to further DDoS attacks. These attacks compromised their ability to conduct business, and their current manually initiated approach was not fully mitigating these attacks.
- **Following the attacks, the customer reviewed various DDoS mitigation providers.** Their requirements included carrier-agnostic and always-on as mandatory features.

AT&T provided the supply chain company with solutions that met the challenge they were facing:

- By providing access to top DDoS technical experts to answer all their questions
- By being able to provide the desired mitigation quickly
- By offering a robust DDoS solution that met their always-on and carrier agnostic requirements

Conclusion

AT&T Cybersecurity played a vital role in bolstering the supply chain company's defensive capabilities against DDoS attacks. The comprehensive solution provided by AT&T addressed the organization's immediate concerns and equipped them with protection against future large volumetric DDoS attacks.