Case Study

Manufacturing

AT&T Cybersecurity

Application layer DDoS attack mitigated with AT&T cybersecurity services

Solutions

- AT&T App and API Protector
- AT&T Content Delivery Network (ACDN) Edge DNS
- ACDN Prolexic DDoS

Highlights

- Customer had an existing denial-of-service solution in place that protected only the transport and network layers (layers 3 and 4) of the IT stack
- The company did not have application layer (layer 7) protection and its web properties were attacked by Russian hackers
- The business was heavily reliant on web-facing properties for commerce
- There were limited IT and budget resources to mitigate the attack
- There was a need for a scalable solution to support the entire IT stack

Overview

A large manufacturing company, heavily reliant on its web-facing properties for commerce, became a victim of an application layer denial-of-service attack. It was targeted by Russian hackers due to sympathies with the Ukraine. The company lost control of its web properties and business and financial operations were impacted. This case study discusses how AT&T Cybersecurity helped the business rapidly mitigate the attack and protect itself from future denial-of-service attacks with a comprehensive full stack DDoS protection solution.

Introduction

The company thought they were protected from DDoS attacks with existing network and transport layer protection. Hackers zeroed in on the unprotected application layer and took down all web-facing properties which impacted day to day business. To remedy the problem, the company needed immediate mitigation of a layer 7 attack to restore web operations.

Initial concerns about budget and limited IT resources were quickly overcome as the company was in the middle of an attack and needed help. They contacted AT&T as their trusted internet provider which coordinated among its sales/technical overlays and partner mitigation team to implement a mitigation solution. This solution needed to be affordable, scalable, and effective to mitigate the attack in order to restore operations.

Key here was availability of Emergency Mitigation services and quick identification of the layer 7 attack to implement AT&T App and API Protector to mitigate the initial attack within 24 hours and to restore web availability. Furthermore, the company realized their exposure and implemented protection across its full IT stack to monitor and mitigate any future attacks.

- AT&T tailored the solution working with customer on multiple off-hour calls
- Edge DNS added to protect against non-existent domain attacks
- Added Prolexic IP Protect as upsell during mitigation to help protect against future attacks

Conclusion

AT&T Cybersecurity played a vital role in mitigating the manufacturing company's denial-of-service attack due to our network relationship. The comprehensive solution provided by AT&T not only mitigated the organization's initial attack but provided a solution for future protection against DDoS attacks.

AT&T provided the manufacturing company with solutions that met the challenge they were facing

Extensive after-hours support at attack peak

Prompt investigation of incident with highly expeditious incident response

Ongoing DDoS protection to mitigate future attacks

Detailed Incident Response Report within 24 hours of initial contact

Addressed limited budget concerns