Pharmaceutical Organization Endures Business Losses Due to Lack of DDoS Protection

OVERVIEW

The Challenge

Organization believed they were not a target of DDoS attacks because they did not transact business through an E-Commerce site and had not been attacked to their knowledge to date.

The Solution

Through data analysis provided by NETSCOUT® solutions the NETSCOUT Team showed the organization the potential risks of nor having DDoS protection in place and the potential value in using a hybrid solution to gain comprehensive DDoS protection.

The Results

A variety of DDoS attacks and indicators of compromise were identified, mitigated and blocked due to implementation of AED and Arbor Cloud®.

Customer Profile

A US based pharmaceutical company that manufactures prescription pharmaceuticals for a range of therapeutic areas including cancer, HIV/AIDS, cardiovascular disease, diabetes and arthritis was looking for a DDoS Protection Solution. Fortunately, they were already a customer of NETSCOUT for Service Assurance and had a trusted relationship with us and one of our partners.

The Challenge

The organization did not have any DDoS protection going into this year and did not believe they had been attacked that frequently. That said, they were hearing about an increase in DDoS attacks targeting peers within their industry. They were also aware that overall DDoS attacks increased 15% this past year and that the volume and size of DDoS attacks increased during the last six months of 2020. However, they didn't feel they needed DDoS protection as a pharmaceutical company because they weren't transacting business on a commercial web site, and they had yet to experience any DDoS extortion attempts against them.

The Solution

In due time, our shared partner made us aware of a small attack that had occurred against one of their data centers. The NETSCOUT Team requested attack data from our ASERT Team to identify the who, what, where, and when of the attack and correlated that data with additional data from the customers ISNG probes to provide a clear picture of the types of attacks that were currently hitting their systems. This analysis helped the NETSCOUT Team display the potential risk to the customer and the value of having some DDoS protection. They also delivered the message that DDoS protection is not just about protecting an E Commerce site but also protecting infrastructure so that the applications and services that use the internet continue to run and be available so their employees who use those applications continue to be productive for the business.

Due to the analysis provided by the NETSCOUT Team the organization was convinced that a cloud solution would protect what they believed needed protection.

Because of the trusted relationship with the customer and the partner the NETSCOUT Team was allowed to do further deep analysis into other areas where attacks to the availability of services could cause issues soon. Because of the ISNG data the NETSCOUT Team were already aware of the companies' network traffic and their traffic patterns and which applications could be vulnerable to an attack. The NETSCOUT Team went site by site in conjunction with the organizations and partners engineering teams to map out the applications that were vulnerable to an internet outage and made recommendations for protection up to management. This further analysis showed that specific types of attacks can slip by a cloud solution and take out a variety of critical services. Some of the attacks that were of concern were application layer attacks that do not trigger volumetric countermeasures or, attacks that can be embedded in encrypted traffic that require decryption to be identified, typically not something cloud solutions provide. More importantly, the team showed management potential Indicators of Compromise (IoCs) within their system that could be communicating with malicious Command and Control Servers out on the internet in preparation for a larger DDoS internal attack or some variety of a Ransomware threat. The identification of these attacks again demonstrated potential risk to the customers networks. The in-depth analysis showed the value to the customer of adopting a hybrid approach to DDoS protection where a cloud solution like Arbor Cloud combined with an on-premise solution like AED is a synergetic relationship that can augment both solutions mitigation capabilities to ensure comprehensive DDoS attack protection with the added capability of blocking outbound threats.

Summary

By proactively employing information readily available through NETSCOUT solutions, the NETSCOUT Team was able to show the customer and partner the potential risks of not having some level of DDoS protection in place. The team was also able to educate the customer and partner on the pros, cons and value of each mitigation strategy so they could make a decision that would provide them comprehensive DDoS protection.

Overarching Benefit

Using NETSCOUT threat intelligence and collected traffic data to illuminate potential cyber-attacks and provide solutions, can help to eliminate likely service outages that could cause productivity and critical business losses.

LEARN MORE

For more information about NETSCOUT solutions visit:

https://www.netscout.com

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECCS_021_EN-2101 09/2021