Global Organization Learns That DDoS Attacks Do Not Stop, and Network Protection Is Critical

OVERVIEW

The Challenge

Attaining an understanding of what is attacking your network is an important factor in understanding how to protect your network.

The Solution

Routine health checks to analyze attack types, duration, complexity and frequency can assist in adjusting protections to be efficient.

Customer Profile

An intergovernmental organization that supports many countries around the world was encountering some DDoS Attack traffic, which threatened their capability to keep services running to their data centers. Because of its global footprint and variety of alliances, they maintain separate and distinct data centers throughout the globe. Due to the size of this IT footprint, the importance of their operation and the diversity of each data center's needs, they approach DDoS Protection with a best-practice hybrid approach including a cloud presence for volumetric attacks and an on-premise presence to protect the edge of the networks from attacks that may get through the cloud solution.

The Challenge

Initially they had seen DDoS attack traffic on their networks and employed several protection strategies including services offered by their ISP as well as a cloud solution to knock down the traffic and protect the services provided to their customers. This approach was somewhat successful, but they did find some attack traffic getting through and becoming a nuisance.

They approached NETSCOUT® to explore our hybrid approach, which would combine a cloud solution to watch for volumetric attacks that would shut down the internet circuits to each of their data centers and on-premise devices, plus would identify DDoS traffic that is designed to evade volumetric attack mitigation. Once in place, they were no longer experiencing the nuisance traffic that would get through previously.

Because they were not seeing the problematic traffic they had seen before, they wondered if it could simply be that the attackers understood that they could not get through and that they were no longer being attacked.

The Solution

During a routine health check by the NETSCOUT team in preparation for a maintenance renewal, they created and presented a report displaying all of the potential attacks that had been identified, mitigated and blocked by the NETSCOUT solution. These attacks comprised volumetric attacks mitigated immediately by the Arbor Cloud installation prior to it getting to the network as well as flood type attacks picked up by Arbor Edge Defense (AED) at the edge of the network prior to getting to the stateful firewalls within the network and shutting them down. More importantly, because of NETSCOUT's Threat Intelligence, AED found and blocked a number of instances where Indicators of Compromise (IOC) embedded in devices through the customer's networks were attempting to communicate with malicious Command-and-Control servers out on the internet. One of these IOCs was the Sunburst malware, which is a trojanized package from the backdoor of the SolarWinds Orion IT Software. If any of these attacks were successful, the customer could have endured substantial downtime, potential data loss and exorbitant network recovery costs.

Summary

Once these attacks were brought to the customers attention, they understood that they would probably be under attack constantly and having a hybrid solution that is designed to identify, mitigate, learn and evolve is what is required to ensure stability and security of business-critical services within all of their disparate data centers.

Overarching Benefit

Understanding that DDoS attacks and cybercrimes are not going away plus having a network protection solution that is comprehensive, agile, efficient, not to mention SMART, is the best solution to keeping your business-critical applications up and running.

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