Intelligently Automating DDoS Response

During a DDoS attack, time is of the essence. A few seconds can mean the difference between a successful mitigation and costly service downtime. Anything that accelerates your mean time to detect (MTTD) and respond (MTTR) to an attack is to your advantage. That makes automation a high priority in the selection of a DDoS defense solution. An intelligent solution can buy you precious time by detecting attacks early and automatically deploying the appropriate countermeasures. But automation must block attacks while not blocking legitimate traffic, and it must inform the operator what was blocked and why. In other words, to be effective it must lead users to the right answer, provide context and supporting analytics and, most importantly, be human-guided – not 'black box'.

Challenge

As DDoS attacks have increased in frequency and complexity, ISP network or security operations teams face an increasing challenge. The latest attack tools can change the attack vectors used within a given attack automatically, every few minutes or seconds, making it necessary for those managing attacks to continuously monitor and tweak their defenses. This increases the operational overhead of the DDoS threat – the number one threat to network availability for ISPs and their customers.

Risk

Black-box automation either works or it doesn't. Every ISP has a different network, they have many different customers with different expectations around DDoS defense, and the DDoS attacks they have to deal with are changing all of the time. Black-box automation is not the answer, as shown by a recent Heavy Reading survey which highlighted the importance of configurability and reporting when customers are looking for automated capability.

Solution

Arbor's Active Threat Level Analysis System (ATLAS®) is one of the world's most extensive threat intelligence gathering platform, delivering near real-time visibility into threat activity across the Internet. More than simply collecting and analyzing data, the Arbor Security Engineering and Response Team (ASERT) curates this threat intel into threat policies and countermeasures delivered via the ATLAS Intelligence Feed (AIF) directly into the Arbor Edge Defense (AED) and Sightline/Threat Mitigation Systems (TMS) intelligent DDoS mitigation systems.

NETSCOUT® has invested in Intelligent Automation. When we automate a process, we allow our automation to be configurable so that our customers can adapt it to their environment and situation. We ensure that the reasons for any automated decisions are clear and logged appropriately giving an audit trail. And, we provide full reporting on the impact that an automated response has to traffic. Arbor Sightline With Sentinel automates DDoS defense in this way, allowing network operators to speed up attack response and reduce the operational overhead plus cost of dealing with attacks.

Summary

Many DDoS solutions on the market rely heavily, if not entirely, on "set and forget" automation that requires extensive baselining and learning yet still cannot distinguish between a genuine attack and a spike in legitimate traffic, and offer little to no attack analytics. The downside of this approach is threefold: triggering false positives, blocking valid customer sessions and no visibility. Automation can put you out in front of an attack and multiply the effectiveness of your security team – but only if it provides the right level of visibility.

It's important to select an intelligent DDoS mitigation solution that can rapidly and automatically distinguish actual attacks from traffic spikes plus dynamically enable and disable the relevant countermeasures as the attack unfolds. It's equally important to have the flexibility to update, reconfigure and refine automated-response capabilities as the sophistication and techniques of DDoS attackers evolves and organizations learn more about the nature of attacks launched against them. Arbor's intelligent countermeasures, near real-time threat analysis and cloud-signaling technologies are based on the industry's most in-depth understanding of DDoS threats, both known and emerging. By capitalizing on these three pillars of DDoS best practices, enterprises and service providers alike can expedite mitigations more effectively and faster than ever.

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

© 2020 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.