AUTOMATION PUTS TIME ON YOUR SIDE IN DDoS ATTACKS

During a DDoS attack, time is unforgiving. A few seconds can mean the difference between a successful mitigation and costly network downtime. Anything that accelerates your mean time to detect (MTTD) and respond (MTTR) to an attack is to your advantage.

That's especially true in today's cloud and enterprise environments, where the combination of greater dependence on internet connectivity and a wider range of security threats can overwhelm network and security operations teams. Security teams, in particular, are under increasing pressure to make critical, on-the-fly judgements about which threats are real and which mitigation measures to deploy — all while the clock is ticking.

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 fundamentally 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'.

ARBOR NETWORKS

The Security Division of NETSCOUT

ARBOR NETWORKS DDoS SOLUTIONS LEVERAGE AUTOMATION IN THREE WAYS

1. Built-In Countermeasures

Arbor Networks APS, our inline, always-on DDoS solution for enterprise and datacenter applications, incorporates more than 30 built-in automated countermeasures, each designed to detect and automatically engage on specific types of attacks based on our deep experience and knowledge of the attack landscape. When APS detects a particular attack, such as a TCP Syn flood, blacklisted hosts or multiple connection attempts from a single host, it will automatically enable/disable the right countermeasures to mitigate those attack types and provide detailed analytics and reporting on the events.

If an attack happens to be in progress when the APS is initially deployed, its countermeasures can still activate immediately because it doesn't require learning times and baselining. Although these built-in countermeasures are designed to work effectively right out of the box, many can also be custom-configured to trigger on the basis of user security policies and risk thresholds.

2. Threat Intelligence Feed

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

The ATLAS Intelligence Feed contains a list of rules associated with different threat types, as well as risk levels (high, medium or low) associated with each type, and is continually updating the Arbor deployment as new threat policies, rules, etc. are developed. If APS, for example, detects suspicious traffic flows that match the active threat policies, it will automatically block the traffic and indicate what it blocked and why in real-time reports.

3. Cloud Signaling

Security experts are increasingly recommending a layered or hybrid DDoS strategy combining on-premises and cloud-based mitigation capabilities for maximum effectiveness. This gives the organization a scalable defense solution that can adapt to different types and sizes of attacks.

The on-premises device can immediately detect and mitigate the majority of smaller-scale, 'low and slow' attacks that typically target firewalls, IPS systems and network perimeter devices whereas larger-scale volumetric attacks are best mitigated at the service provider level in the cloud. But thwarting these multi-layer attacks requires the two defensive components to work in synchronization.

Cloud Signaling is Arbor's mechanism by which the on-premises component (Arbor APS) communicates in real-time with the service provider's cloud component (SP/TMS, Arbor Cloud) to synchronize this mitigation action. If attack volume at the premises level escalates to a user-specified threshold, Cloud Signaling can automatically trigger the cloud mitigation countermeasure(s) and share attack data such as blocked IPs. Security operators can also initiate Cloud Signaling manually when they see a growing threat. Arbor's hybrid solution allows network and security teams substantial flexibility to configure and fine-tune their Cloud Signaling policies.

INTELLIGENT COUNTERMEASURE AUTOMATION

It's all about speed of detection and mitigation. 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.

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 in many cases, and offer little to no attack analytics. The downside of this approach is threefold: triggering false positives, blocking valid customer sessions and no visibility.

It's important to select an intelligent DDoS mitigation solution that can rapidly and automatically distinguish actual attacks from traffic spikes and dynamically enable/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.

Click here to learn more about Arbor's DDoS solutions.

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

AI/DDoSAUTOMATION/EN/1117-LETTER

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

North American Sales
Toll Free: +1 855 773 9200

Europe
T: +44 207 127 8147

Asia Pacific
T: +65 6664 3140

Latin & Central America
T: +52 55 4624 4842