CLOUD SIGNALING

For nearly a decade, DDoS (Distributed Denial of Service) was a basic flood attack that simply tried to overwhelm a network connection with excessive traffic. The goal: take the target offline. Early on, DDoS was a brute force attack against availability.

Beginning in 2010, and driven in no small part by groups like Anonymous and the rise of Hacktivism, we saw a renaissance in DDoS attacks that led to innovation in the areas of tools, targets and techniques.

Seemingly overnight, DDoS attacks were targeting not just connection bandwidth, but multiple devices that make up existing security infrastructure. 0This included Firewalls and IPS devices, as well as a wide variety of essential applications that run on HTTP, HTTPS, VoIP, DNS and SMTP.

These new attack vectors required a new kind of protection. Alarmingly, there was no comprehensive threat resolution mechanism to adequately address application-layer DDoS attacks at the data center edge. Nor were there sound approaches to dealing with volumetric DDoS attacks in the cloud. While many data center operators had purchased DDoS protection services from their ISP or MSSP, they lacked the ability to seamlessly connect on-premise and cloud mitigations.

Arbor's Innovation

Arbor set out to solve this challenge by developing an automated and real-time solution that integrates mitigation of application-layer attacks at the customer edge with volumetric attacks upstream.

Now, when an enterprise or data center operator discovers that they are under a service-disrupting DDoS attack, they can choose to mitigate the attack in the cloud simply by clicking on a drop-down menu and triggering an alert to the service provider. The signal can also be set at a predetermined capacity level for more automated protection. As a result, a volumetric DDoS attack that attempts to congest the upstream links would immediately be neutralized from affecting the data center's access links. The net effect: service availability remains uninterrupted.

ARBOR NETWORKS
The Security Division of NETSCOUT

"Cloud Signaling has been a key innovation in enabling the industry-wide adoption of hybrid, or multi-layer DDoS defense as a best practice. Arbor understands the threat landscape and created an elegant way of linking on-premise and cloud-based mitigation. This tight connection is key to delivering protection from today's advanced DDoS attacks."

Because Cloud Signaling has emerged as a best practice for DDoS protection, Arbor has opened its Patent for Cloud Signaling. This proven methodology empowers the industry to develop a standard approach to multi-layer protection. The IETF is working on DOTS, DDoS Open Threat Signaling, "a method by which a device or application may signal information relating to current threat handling to other devices/applications that may reside locally or in the cloud."

Arbor's Cloud Signaling innovation has brought a new level of protection to businesses around the world and is now an essential component of best practice DDoS defense.

AI/CLOUDSIGNALING/EN/0917-LETTER

ARBOR NETWORKS
The Security Division of NETSCOUT