radware

Guide

Smart DDoS Protection During the COVID-19 Crisis

The ongoing effects of the coronavirus pandemic are creating a significant impact on businesses worldwide. While some industries have been severely hit, others are experiencing sudden and exponential growth in demand for their services.

Sadly, this difficult time offers no reprieve from cybercriminals who are using this crisis as an opportunity to attack critical infrastructure. With customers, patients and citizens relying on critical services now more than ever, these attacks emphasize the importance of protecting infrastructure and ensuring service availability.

As organizations are adjusting to these challenging times, they need to make sure they are adapting their security as well. This includes increasing protection capacity to ensure the surge in legitimate traffic is secured, safeguarding remote access infrastructure through virtual private networks (VPNs) and Remote Desktop Protocol (RDP), and protecting cloud-based environments which are being quickly scaled up due to increasing demand.

Five Critical Capabilities for Protection During the COVID-19 Crisis

BEHAVIORAL-BASED DETECTION

As spikes in traffic for videoconferencing, telemedicine and governmental websites show, organizations need a way of distinguishing between malicious traffic and legitimate traffic spikes. During periods of massive flash crowds, it is critical that your distributed denial-of-service (DDoS) defenses leverage behavioral-based detection methods to distinguish between attackers and legitimate users.

REAL-TIME SIGNATURE CREATION

It is critical that DDoS defense signatures are tailored to the exact characteristics of incoming attack traffic. If you apply a signature too narrowly, no attack traffic will be stopped. If you apply a signature that is too broad, legitimate user traffic will be blocked. A traditional DDoS solution relying on rate limiting will not be able to distinguish between legitimate and attack traffic.

ENCRYPTED ATTACK PROTECTION

More than 90% of web traffic is now HTTPS encrypted. While HTTPS is crucial for data protection, it opens the door for new DDoS attacks. HTTPS requires many more resources from the target server than the client, meaning hackers can unleash devastating attacks with limited requests. Protection against encrypted DDoS floods is a critical requirement for modern DDoS protection.

MASSIVE GLOBAL CAPACITY

Internet of things (IoT) botnets are growing larger and more sophisticated and becoming more capable of launching larger attacks. They can be purchased on the darknet for relatively small sums. Botnets are a significant threat during a massive public health emergency such as the COVID-19 crisis. Therefore, a globally distributed DDoS scrubbing network with multiterabit DDoS scrubbing capacity is critical for protection.

MANAGED SECURITY SERVICES

Staff shortages and the cybersecurity skill gap are crucial problems, but they become exacerbated during a crisis when IT teams are overextended and many employees work remotely. Using a fully managed security service for DDoS protection takes the burden off your shoulders by relying on network and application security experts.

Radware's Cloud DDoS Protection Service

Radware is the industry leader in DDoS protection, providing comprehensive Layer 3–7 protection against DDoS attacks and ensuring service availability. Radware's DDoS protection solutions can be deployed through an on-demand service, always-on service or hybrid service combining cloud service with a hardware appliance.

Radware's Cloud DDoS Protection Services are deployed atop a global scrubbing network with dedicated, multi-terabit scrubbing capacity and supported by Radware's Emergency Response Team (ERT), guaranteeing customers full protection and peace of mind during this challenging time.

Key Features of Radware's Cloud DDoS Protection Service:

Behavioral-Based Detection to distinguish between legitimate and malicious traffic

Massive Global Network with 11 scrubbing centers and 5Tbps of dedicated scrubbing capacity

Real-Time Signature Creation to automatically tailor defenses within 18 seconds or less

Fully Managed Security Service supported by Radware's Emergency Response Team (ERT)

Advanced Attack Protection against sophisticated vectors such as Burst attacks, IoT botnets, Dynamic IP, etc.

Robust Management Portal with extensive visibility, reporting and self-service options

Smart SSL Protection to stop attacks without adding latency or violating user privacy

Industry-Leading SLA with six granular, measurable metrics to verify service performance

DDoS Mitigation Scrubbing Center

11
scrubbing centers worldwide

5Tbps
of global mitigation capacity

Unmatched
ability to guarantee long-term DDoS mitigation capabilities