Web DDoS Protection

Safeguard your business in today's evolving threat landscape.

Shifting Landscape:

The new web DDoS tsunami threat

Recent attack campaigns show cybercriminals leveraging multiple types and vectors of attacks as part of single campaigns, combining both network and application-layer attack vectors and leveraging new tools. As a result, they've created sophisticated new attacks that are harder, and sometimes impossible, to detect and mitigate with traditional methods.

Web DDoS Tsunami attacks, an extreme form of HTTP/S flood attack, are characterized by high volume with skyrocketing levels of requests per second (RPS). They are encrypted and appear as legitimate requests. They also leverage sophisticated evasion techniques to bypass traditional application protection. These techniques include randomizing HTTP methods, headers and cookies; impersonating popular embedded third-party services; spoofing IPs and more. Among the application-level attack methods seen in recent campaigns were HTTPS Get, Push and Post request attacks with changing parameters behind proxies and dynamic IP attacks. All look like legitimate requests.

A New Offering for This Emerging Threat

Unique Attacks Require Dedicated Protection

Existing protection mechanisms are not always able to detect and mitigate Web DDoS Tsunami attacks due to their sophistication and complexity. A new and separate module is necessary to combat these unique assaults in a dedicated way. Our Web DDoS Protection, whether in add-on or subscription, bridges this gap and ensures that you stay ahead of the curve.

Tailored Defense: A New Service Module

Radware has invested substantial resources in research and development to address the sophisticated attacks that differ from regular Layer 7 attacks. Although the attacks can reach several million RPS, they are analyzed by our AI-based algorithms to generate accurate real-time signatures in seconds. Our dedicated team has crafted a whole new service module and algorithm specifically tailored to counter these threats. This technology safeguards your critical assets by focusing on the intricacies of Web DDOS Tsunami attacks.

Scaling Up Responsibly: Heavy Compute Resources

The sheer scale of Web DDoS Tsunami attacks demands robust computational power. Our solution is meticulously designed to handle this immense load. However, such comprehensive protection requires heavy compute resources. The signature that is based on dozens of HTTP parameters requires large scale of processing. To maintain optimal performance, we've separated this specialized defense layer from the existing service scope. By doing so, we ensure that your core services remain unaffected while providing targeted protection against Web DDoS threats.

Fortify Your Defenses

Web DDoS Protection is not just a prudent choice; it's a strategic imperative. By securing your digital infrastructure against the evolving threat landscape, you safeguard your reputation, customer experience and bottom line. Let Radware be your shield in this cyber battleground, ensuring uninterrupted services and peace of mind.

For inquiries or to activate Web DDoS Protection, contact Radware today.

RWI-228 | 03.20.2024