RADWARE PROTECTS MAJOR ONLINE BUSINESS AGAINST PERSISTENT WEB DDOS ATTACK CAMPAIGN

A Massive, Complex, and Persistent Web DDoS Attack

Over the recent week, Radware has been protecting a major online business against a persistent, massive, and complex Web DDoS Tsunami attack campaign.

This major online business was initially the target of an online 'hacktivist' group. However, as time went by, the political motivation has been replaced by financial aspirations, and the customer was facing DDoS ransom demands of millions of dollars.

There are several aspects to this attack campaign which make it unique:

- **PERSISTENCE OF ATTACK**: this is a very persistent attack campaign, ongoing for nearly a week, by now. Already Radware has observed nearly 20 different attack waves.
- **MASSIVE ATTACK WAVES**: each of the attack waves was very large, with some of the attack waves peaking at nearly 2 million Requests per Second (RPS).

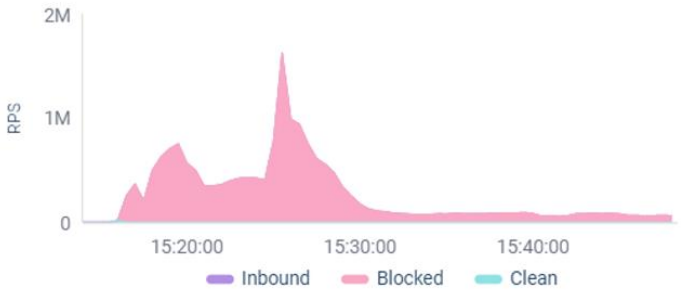

Figure 1: *Attack wave peaking at nearly 2 million RPS*

- **LONG DURATION OF EACH WAVE**: combined with the large peaks, the attack waves also tended to be very long, with some lasting several hours. All in all, some attack waves reached over 10 billion requests in aggregate.

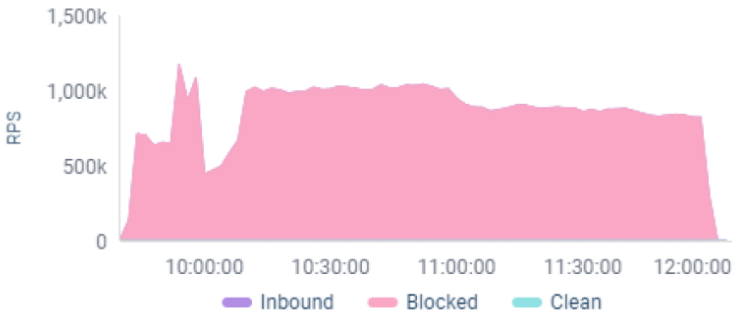

Figure 2: *Persistent attack wave of over 1 million RPS for almost 3 hours*

- **COMPLEXITY OF ATTACK PATTERN**: the attacks were crafted as HTTPS GET requests, masquerading as legitimate web requests. The attackers used a complex attack pattern, which made it particularly difficult to distinguish from legitimate traffic. As a result, any type of protections based on pre-existing signatures or rate-based detections could not protect against this attack.

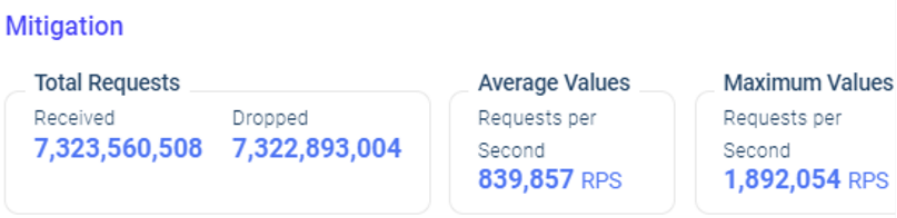

***Figure 3**: Aggregate data from one of the attack waves, peaking at over 1.8 million RPS and receiving in total over 7 billion requests*

Radware assisted the organization with emergency onboarding to Radware's Cloud Web DDoS "Protection Service. Even without a learning period, Radware's real-time signature-creation algorithms automatically created and applied custom signatures, tailored to the specific characteristics of this attack, and was able to accurately mitigate these attacks without blocking legitimate traffic.

Radware's Emergency Response Team (ERT) also worked with the customer to fine-tune protections, and make sure that no false positives were generated. As a result, the ongoing attack waves are being mitigated in full, with no impact to users.

If you are facing a Web DDoS attack, contact Radware immediately for emergency onboarding to our DDoS protection services.

Radware Under Attack Contact Page:

https://www.radware.com/underattack/