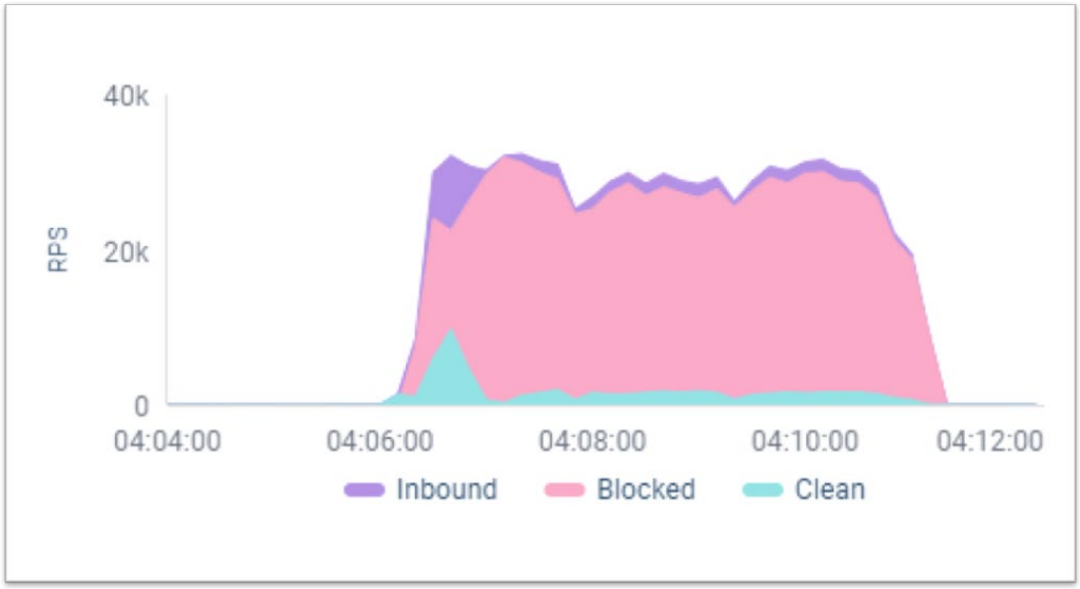
Radware Protects European Hospital Network From Web DDoS Attack Campaign

Radware recently protected a large European hospital network from a persistent, massive and complex Web DDoS Tsunami attack campaign.

The hospital network, which features more than 30 hospitals and medical facilities and serves more than 10 million patients annually, became a target when an international hacktivist group began to focus on medical facilities within the country. As a result, the healthcare network's applications were attacked repeatedly over a period of six weeks.

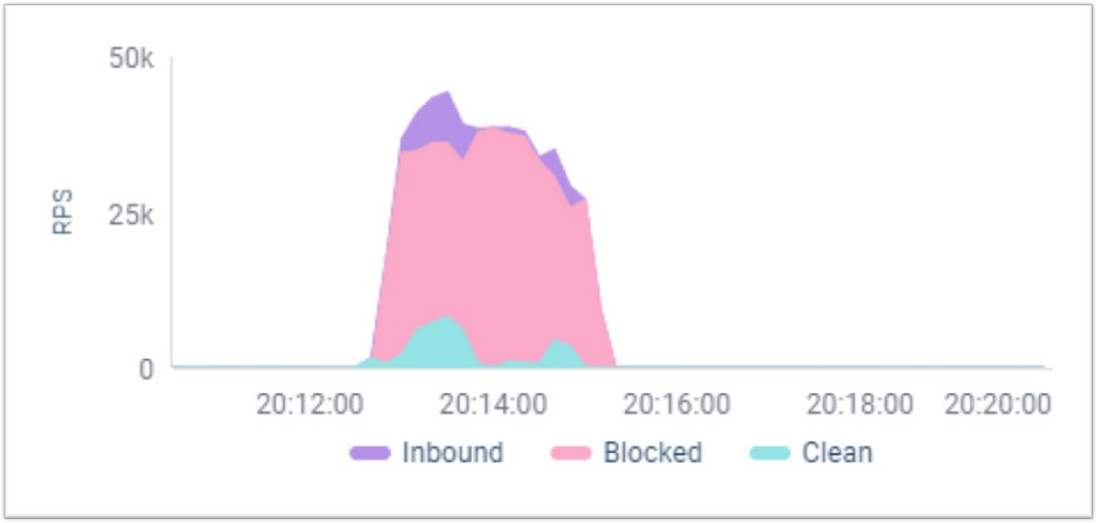
Figure 1:
A 7-minute attack wave peaking at nearly 40k RPS



Several aspects of this attack stand out:

- **Persistence of Attack Campaign:** The healthcare provider was targeted by nearly a dozen major waves for a period of six weeks.
- **"Hit and Run" Burst Attacks:** The attacks consisted of short bursts under 10 minutes long with 30-50 thousand requests per second (RPS) each.

Figure 2:
A 5-minute attack wave peaking at nearly 50,000 RPS



- **Attack Pattern Randomization:** Each attack wave pattern was varied, requiring a different defensive signature to mitigate. This required a high degree of automation to dynamically adapt the signature to the attack pattern.
- **Complexity of Attack Pattern:** The attacks were crafted as HTTPS GET requests, masquerading as legitimate web requests. The attackers used a complex attack pattern that made it particularly difficult to distinguish from legitimate traffic. As a result, any type of protection based on pre-existing signatures or rate-based detections could not protect against this attack.

Radware assisted the organization with emergency onboarding to Radware's Web DDoS "Under Attack" mode. 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.

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

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

Contact us

RW-1231 8.22.2023