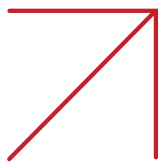




Radware Protects Online Business Against Persistent Web DDoS Attack



Over the recent week, Radware recently protected a major online business against a persistent, massive and complex Web DDoS Tsunami attack.

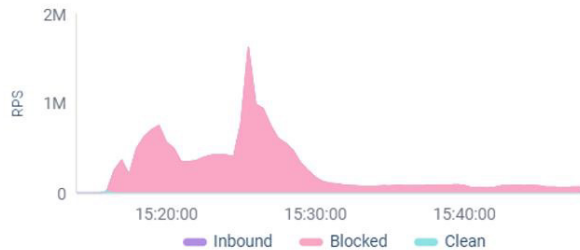
This major European online business was initially the target of an online hacktivist group. However, as time went by, the political motivation has been replaced by financial aspirations, and the customer now faced DDoS ransom demands on millions of dollars.

There are several aspects to this attack which made it unique:

- **Persistence of Attack:** This is a very persistent attack campaign, ongoing for nearly a week. 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:

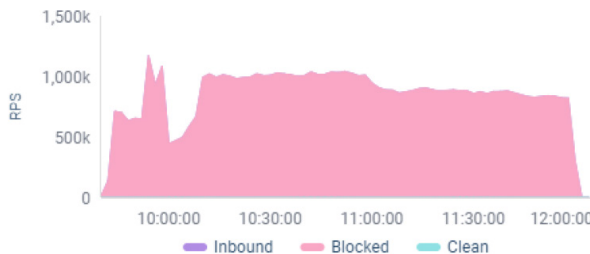
Attack wave peaking at nearly 2 million RPS



- **Long Duration of Each Wave:** Apart from 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

Mitigation

Total Requests

Received **7,323,560,508** Dropped **7,322,893,004**

Average Values

Requests per Second **839,857 RPS**

Maximum Values

Requests per Second **1,892,054 RPS**

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 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/>

About Radware

Radware® (NASDAQ: RDWR) is a global leader of [cybersecurity](#) and [application delivery](#) solutions for physical, cloud and software- defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com. Radware encourages you to join our community and follow us on: [Radware Blog](#), [LinkedIn](#), [Facebook](#), [Twitter](#), [SlideShare](#), [YouTube](#), [Radware Connect](#) app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

©2023 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.

