

- Radware Insider - <http://insider.radware.inside/wordpress> -

Radware Protects Major Stock Exchange Under Anonymous Attack

Posted By [sergeyg](#) On November 3, 2011 @ 2:25 pm In [Security](#) | [No Comments](#)



A major stock exchange (SE) experienced multi-vulnerability cyber attack campaigns that aimed to shut down its web site. Radware stepped in and mitigated all attacks effectively, assuring the SE site stayed on-line in spite of the attacks.

Radware Helps Stock Exchange Defend Against Anonymous Attack

On October 10th, hacktivists carried out their threat on the SE's main website with several denial of service attack tools that were effectively mitigated thanks to a joint effort by the SE's network security team, Radware US security team, and Radware ERT.

Invoking Radware ERT

The SE was not a Radware security customer, so the American sales and sales engineer teams contacted SE and offered our Attack Mitigation System (AMS) with local support of the US-based team and remote support of ERT. Out of several vendors offering protection solutions, SE selected Radware. This is an indication of the favorable reputation Radware has gained in mitigating DDoS attacks.

Attack Topography

Attacks witnessed and mitigated by deployed Radware DefensePro devices (October 10, 2011) include:

1. Oversized UDP Frame Flood (over 1Gbps)
2. Multiple LOIC DDoS Tool TCP attacks Multiple LOIC DDoS Tool UDP attacks Multiple Mobile DDoS LOIC (HTTP flood)
3. Multiple UDP Floods on port 80, on port 53 and random ports (300 Mbps+)
4. #Refref DDoS Tool attacks (home grown by Anonymous – first time witnessed!)
5. TCP Fragment Floods

These attacks were mitigated, and the devices downstream did not experience any issues. Examples of the attacks and how the Radware AMS mitigated these attacks are shown below. The **Blue** line in the traffic graphs indicates the traffic being received inbound, and the **Red** line indicates the attack traffic detected, blocked and discarded.

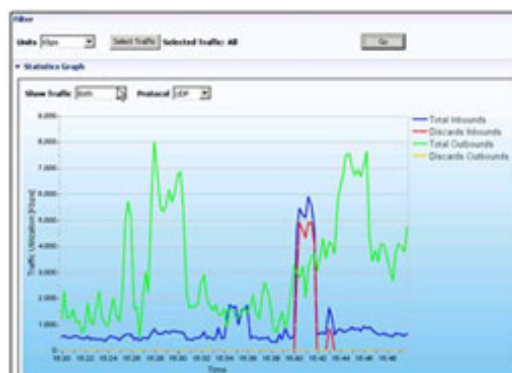


Figure 1: UDP Flood at 15:30 EDT 1

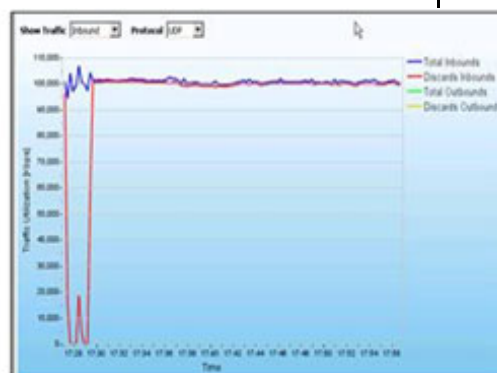


Figure 2: UDP Flood at 17:30 EDT 1

To effectively protect against all of the above attacks, one needs to employ multiple network security technologies: DoS Protection, Network Behavioral Analysis (NBA) and Intrusion Prevention (IPS).

Account manager: Myles Moskowitz, Major Accounts Manager, Radware Inc.

Security engineering team:

1. Carl Herberger, V.P. Security Solutions, Radware Inc.
2. Raj Vadi, Director, Scalable Systems Architect, Radware Inc.
3. Dennis Usle, Security Solutions Architect - East, Radware Inc.

ERT: Ziv Gadot, ERT & SOC team leader.

Ron Meyran, Director Product Marketing – Security

Article printed from Radware Insider: **<http://insider.radware.inside/wordpress>**

URL to article: **<http://insider.radware.inside/wordpress/?p=5243>**

Copyright © 2008 Radware Insider. All rights reserved.