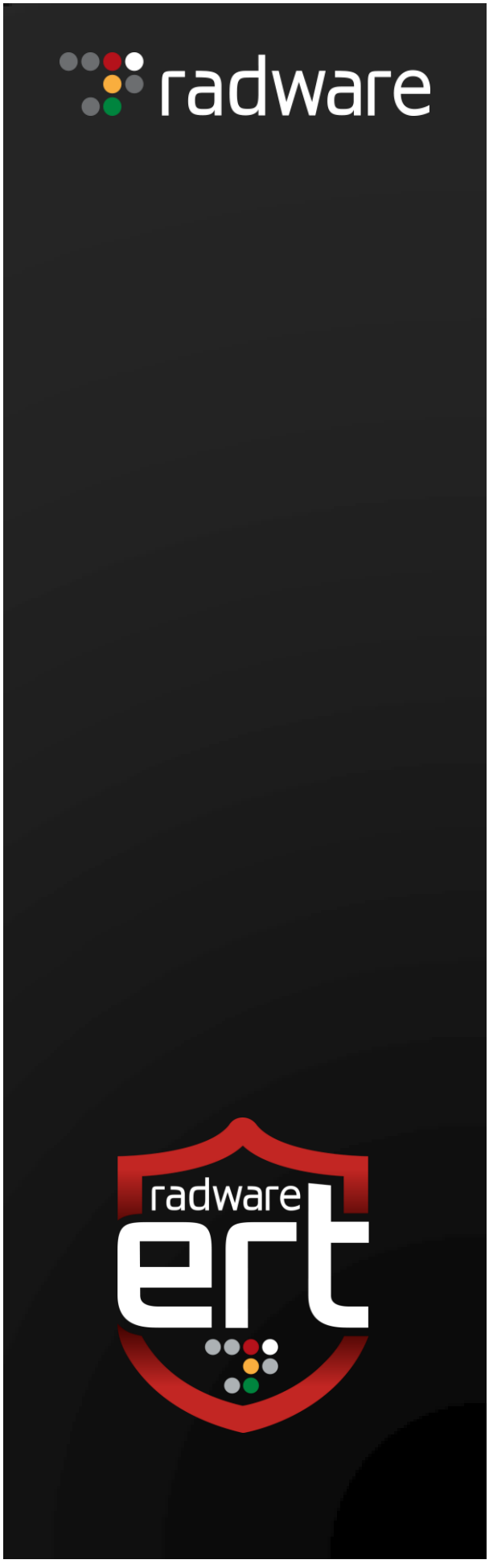


ERT THREAT ALERT

#OpSaveGaza July 11, 2014

Introduction

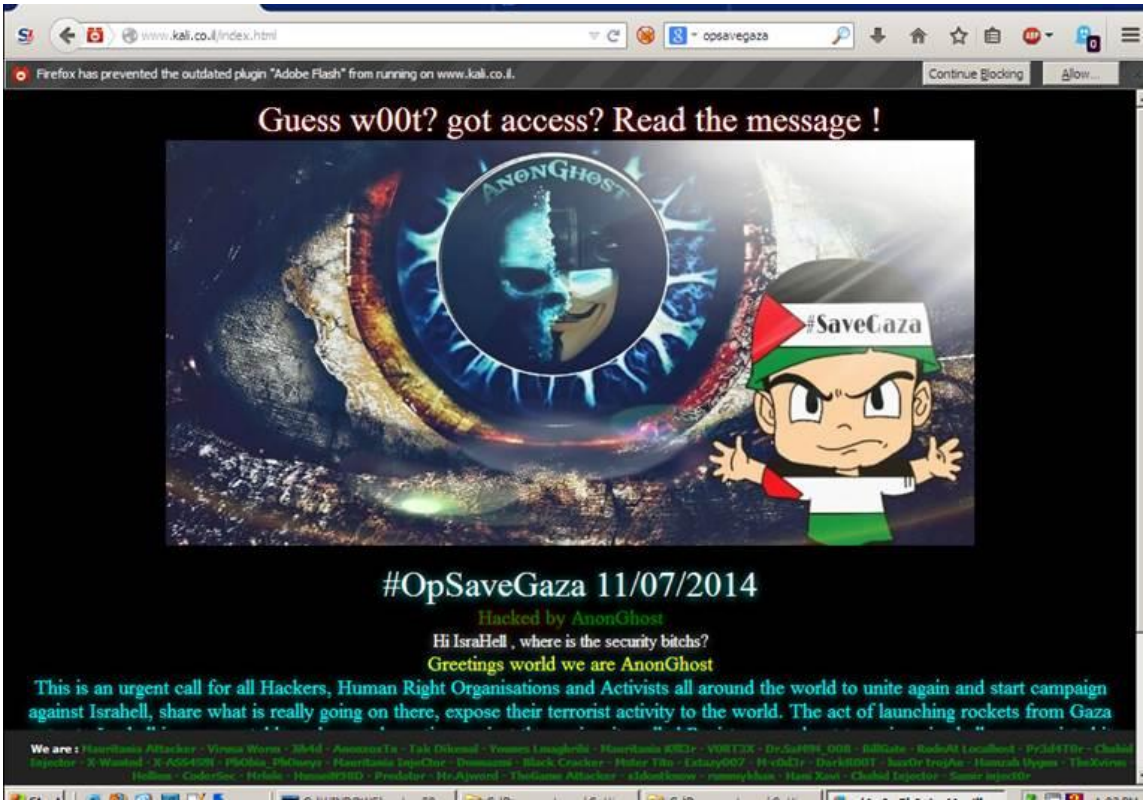
Due to the growing tension between Palestine and Israel that includes military actions in the sector of Gaza, several hacktivists groups have united in a cyber-attack campaign against Israel, named #OpSaveGaza.

From information that was found online (Twitter #OpSaveGaza and Facebook), AnonGhost and other hacktivist groups claim to have successfully defaced over 500 Israeli websites and leaked some government email credentials. In addition, some government sites have been targeted for DDoS attacks.

A link to DoS tools on the #OpSaveGaza page indicates a few of the tools that will be used. Most of them are known, such as HOIC, LOIC and ByteDos.

Radware's Emergency Response Team (ERT) has not yet directly seen any cases related to this activity.

Here is example of kali.co.il which was recently defaced. Kali is an Israeli-based company that provides financial services.



General Recommendations

1. Organizations under threat should revisit the following protections that are relevant to this operation:
    a. Protection against application DoS attacks
    b. Protection against network attacks, especially volumetric attacks that can saturate the Internet pipe
    c. Protection against low-and-slow DoS attacks
    d. Protection against web site intrusion, to prevent defacement and information theft

2. Monitor security alerts—examine alerts and triggers carefully. Fine-tune existing polices and protections to prevent false positives and allow you to identify real threats if and when they occur.

Recommendations for Radware Attack Mitigation Network (AMN)) customers

1. Revisit the following protections and ensure they are turned on and in “block on” mode. These are primary features to be used against the attacks:
    a. Behavioral DoS
    b. SYN protection
    c. Web challenges
    d. IPS signatures — make sure your signature is up-to-date (at least 0009.0253.00 or above)
    e. DefensePipe

Note: Radware ERT recommends that any configuration changed should be carefully reviewed and conducted in the proper manner.

2. Take capture files during an attack (either from the DefensePro product or external device)

3. If any attack is not mitigated well, contact Radware ERT.

Recommendation for non-Radware customers

1. To understand how Radware solutions can better protect your network, contact us here.

2. If your organization is under attack, immediate help is available from Radware’s ERT. Follow the instructions at ‘Under Attack’ in the following page.