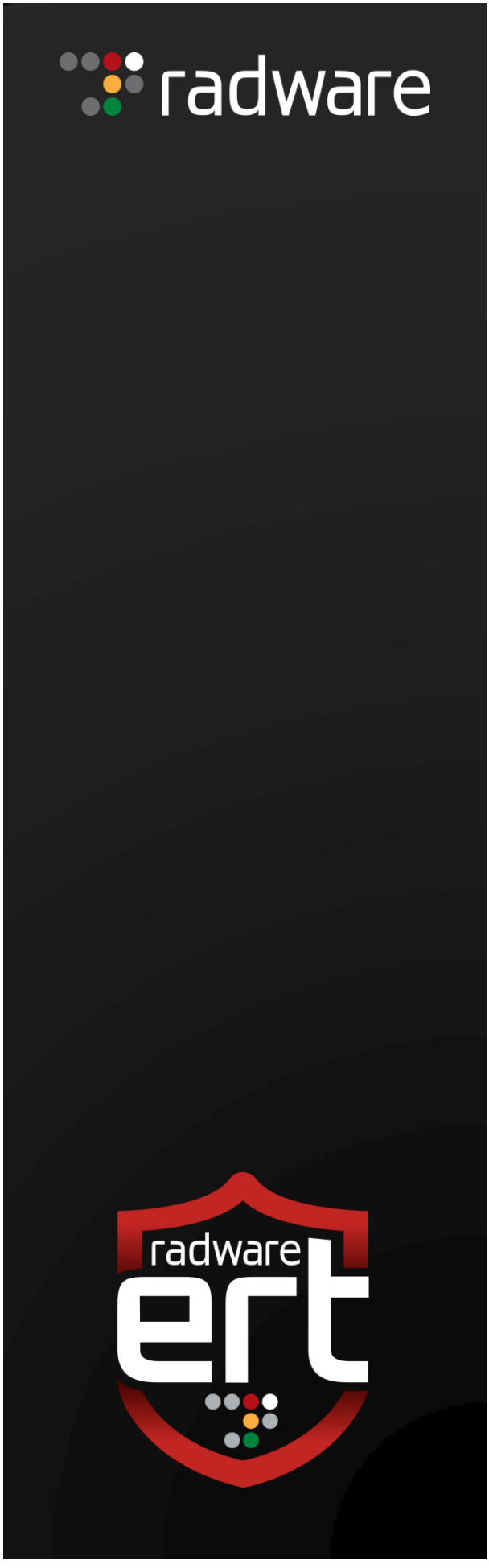

ERT THREAT ALERT

OpIsrael
April 7, 2015

Introduction

OpIsrael 2015 is an organized set of attacks aimed at the Israeli government, public institutions and other high profile Web sites. These attacks are planned by anti-Israeli individuals and Anonymous-affiliated hacktivist groups such as “AnonGhost” (Tunisia). The goal of the attackers is to a launch a massive set of cyber-attacks against Israeli cyber space. OpIsrael 2015 is the third in a series of OpIsrael attacks – with the first occurring in 2013.

This document provides guidance for preparing and recommendations to reduce the vulnerabilities for sites at risk.

Figure 1 – OpIsrael Banner

Technical Details

Although there is no definite information about the attack content (which is typical with broad types of attacks), multiple attack tools and techniques are expected - including intrusion attempts, information theft and DDoS. There are however two tools which were mentioned more frequently than others:

Doser 2.0

Doser 2.0 is a traffic generator with scanning capabilities using multiple threads and sockets. Its attack vectors include:

- TCP flood
- UDP flood
- HTTP flood

These DOS/DDOS tools and methods are published and distributed to the general public in an effort to create large scale DOS/DDOS attacks with as many participants as possible worldwide.
In addition to the amateur participants, there is a fraction of individuals/hack groups with higher capabilities that are able to perform advanced attacks on specified targets using Trojan horses, worms, brute force, CSS, SQL injections and other advanced hacking methods.

Anonymous External Attack

Anonymous External Attack is tool develop by AnonGhost and likely to be used in OpIsrael 2015 (run by AnonGhost). The tool generates a UDP Flood with payload containing multiple zeros, by default against port 80. The tool can be blocked, among other technique, by blocking the UDP traffic to the targeted port.

Related links

#OpIsrael - Twitter

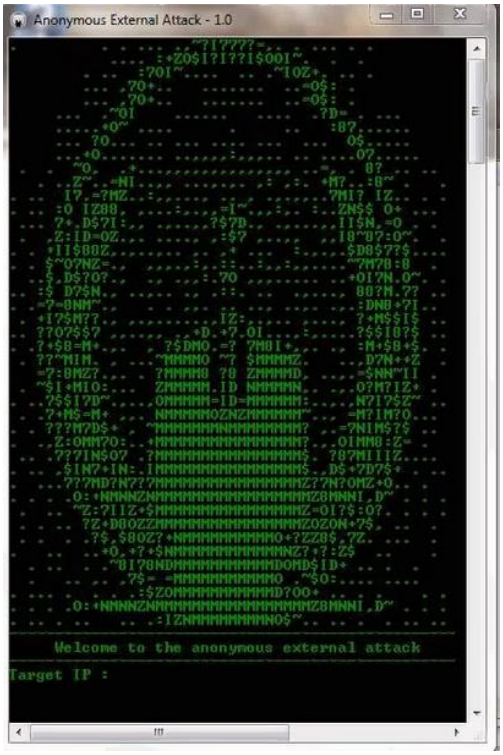

Figure 2 – Anonymous External Attack

General Recommendations

Organizations under threat should revisit the following

- Protection against application DoS attacks
- Protection against network attacks especially volumetric attacks that can saturate the Internet pipe
- Protection against low-and-slow DoS attacks
- Protection against web site intrusion to prevent defacement and information theft

Monitor Security Alerts

Examine alerts and triggers carefully. Tune existing polices and protections to prevent false positives and allow identification of real threats if and when they occur.

Recommendations for Radware Attack Mitigation Network (AMN) Customers

Revisit the following protections to ensure they are turned on and in-block is on. These are primary features to be used against the attacks:

- Behavioral DoS
- SYN Protection
- Web Challenges
- IPS Signatures- make sure signature is up-to-date (at least 0009.0253.00 or above)
- DefensePipe

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

- Take capture files during an attack (either from the DefensePro product or external device)
- Contact Radware's ERT if any attack is not mitigated well

Recommendations for Non-Radware Customers

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

If you are under attack and require expert emergency assistance from Radware's ERT, contact us with the code "REDBUTTON."