DoS Cyber Attack on a Government Agency in South America- February 2012

Anonymous' Mobile LOIC in Action

Table of Content

Preamble **3**

About Radware's DefensePro 3

About Radware's Emergency Response Team 3

Attack summary **4**

Executive Summary 4

Attack Vector Details **5**

Attack Vector I: HTTP Flood: Mobile-LOIC 5

Attack Vector II: TCP Data Flood: LOIC 6

Attack Vector III: UDP Floods 7

Attack Vector IV: HTTP Flood: other tools 8

Geographical Blocking **8**

Preamble

This attack case summary describes one of the real life attacks which was experienced by a Radware customer and successfully mitigated thanks to Radware's DefensePro product and Radware's Emergency Response Team (ERT) expertise. The customer's name is undisclosed for privacy purposes and is referenced by "customer" in this report.

About Radware's DefensePro

Radware's award-winning DefensePro is a real-time network attack prevention device that protects the application infrastructure against network & application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft and other emerging network attacks. It combines a set of security modules which altogether provide a complete attack mitigation solution: Intrusion Prevention System (IPS), Network Behavioral Analysis (NBA), Denial-of-Service (DoS) Protection and Reputation Engine. The vast majority of the attacks are successfully mitigated and stopped by DefensePro alone.

About Radware's Emergency Response Team

Radware's Emergency Response Team (ERT) is a service, complementary to Radware's DefensePro, designed to provide 24x7 security services for customers facing a denial-of-service (DoS) attack or a malware outbreak. Often, these attacks require immediate assistance. The ERT provides instantaneous, expert security assistance in order to restore network and service operational status. IT is staffed by experts that have vast knowledge and experience with network threats, their detection and mitigation, and in-depth experience of the DefensePro family of products. In addition, the ERT takes information from each customer engagement and simulates the same scenario internally for further analysis and proactive implementation of defense techniques for other customers that may be facing a similar security threat.

Attack summary

Executive Summary

The customer, a high-profile Government entity, was targeted by a DDoS attack in the context of a wider campaign against Government sites in this country.
In the days preceding the attack, Anonymous published warnings and threats of attacks through their usual means of communication (Youtube, Twitter, Facebook).
The site was protected by a DefensePro device, just installed and configured few days ago. ERT, which was invoked, logged in on the day of the attack to tune the device which successfully mitigated the attack and the website was available to users.
This document describes different attack vectors and their mitigation and discusses the effectiveness of Geo-Blocking, used by the customer during the attack.

Attack Vectors

There were four confirmed attack vectors in this attack campaign:

Attack Vector I: HTTP Flood: Mobile-LOIC
Attack Vector II: TCP Data Flood: LOIC
Attack Vector III: UDP Floods
Attack Vector IV: HTTP Flood: other tools

Attack Vector Details

Attack Vector I: HTTP Flood: Mobile-LOIC

Summary

Using the Mobile-LOIC attack tool, each attacker sent multiple HTTP GET requests to the customer's webserver home page. Mobile-LOIC delivers semi-random parameter values in its requests in order to evade proxies and caching services and reach the backend server. DefensePro blocked this attack vector using an Application Security signature.

Mobile-LOIC Control Panel

Attack Description

Verified attackers: about 100

TPS: ~400

Bandwidth: 1.5 Mbps

HTTP GET requests for the homepage ("/"), two parameters were delivered in the URL:

id= Semi-random 13 digits number

Attack packets snapshot

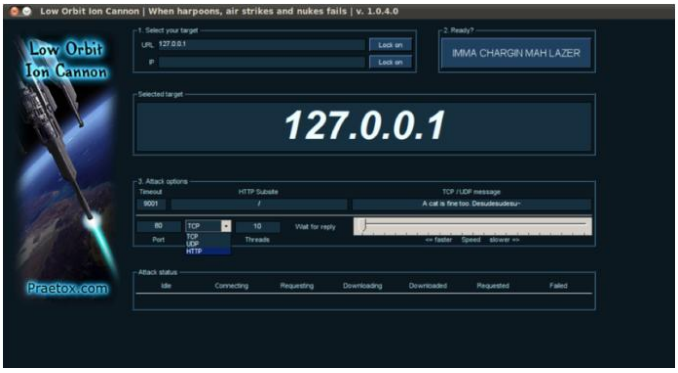
One of the problems of HTTP flood attacks (from attacker's perspective) is that HTTP request may be answered by the local ISP proxy or by CDN, and not reach the actual targeted web server. Mobile-LOIC uses the Random Parameters technique in order to create un-cacheable requests, ensuring each will reach the backend server.

Attack Vector II: TCP Data Flood: LOIC

Summary

Using the LOIC attack tools, attackers sent multiple TCP data packets with constant payload toward TPC/80 at the attacked Webserver. This attack vector was not substantial and only few attackers used it.

DefensePro blocked this attack vector using two Application Security signatures.



LOIC Control Panel

Attack Vector III: UDP Floods

Summary

The third attack vector was: UDP Floods. The device blocked several of them during the length of the campaign using the Behavioral DoS Protection and the Black List; this includes floods on UDP/80 and UDP/443 and Fragmented UDP flood on random destination ports.
Some of the floods were probably generated using LOIC.

Attack Description

The following UDP floods were detected and blocked by DefensePro device:

- 33K PPS UDP/80 flood, probably generated using LOIC
- dd4K PPS 45 Mbps Fragmented UDP flood, random destination port
- Low rate UDP/443 flood

Attacking sources were almost certainly spoofed by the attackers.

Attack Mitigation

Attacks were mitigated using a combination of Behavioral DoS, DoS-Shield signature for Fragmented Flood and Black List on UDP/80 and UDP/443.

Attack mitigation

Attack Vector IV: HTTP Flood: other tools

Summary

Additional HTTP GET Request floods generated by other attack tools (HOIC for example) were blocked using the Web Cookies challenge mechanism. No additional information is currently available.

Geographical Blocking

During some stages of the attack, the customer blocked requests originating outside the customer's country at the ISP level. This technique achieved only limited outcome since some attacker sources were originating **at the customer's country itself.**
The following map shows countries where attack traffic originated: