radware
Smart Network. Smart Business.

ERT Attack Report

DoS Cyber Attack Campaign Against Israeli Targets

April 7-9th, 2013

Table of Contents

Executive Summary

On April 7th, a Radware customer was targeted with DoS attacks assembled by the Anonymous group as part of an attack campaign on the Israeli cyberspace.

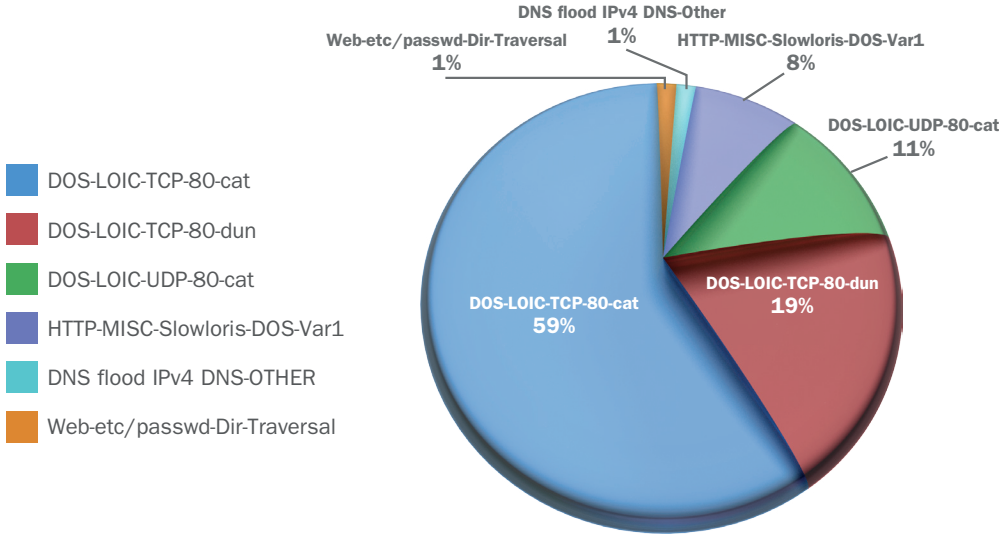
The focus of this report is to analyze the attack on the customer's networks and clients, while examining the magnitude of the attack. The report contains the attack vectors and tools that were used against the customer's network based on ERT's analysis.

When analyzing the reports generated by DefensePro units installed on customer premises, ERT took a top-down approach, focusing on the most prominent attacks observed by bandwidth and number of incidents.

Known Attack Tools

Attacks were dissected by the number of independent attack triggers reported by DefensePro per known attack tool. From the graph below, we can see the most used attack tools. At the time of the attack, LOIC (both TCP and UDP attack vectors), and Slowloris were used.

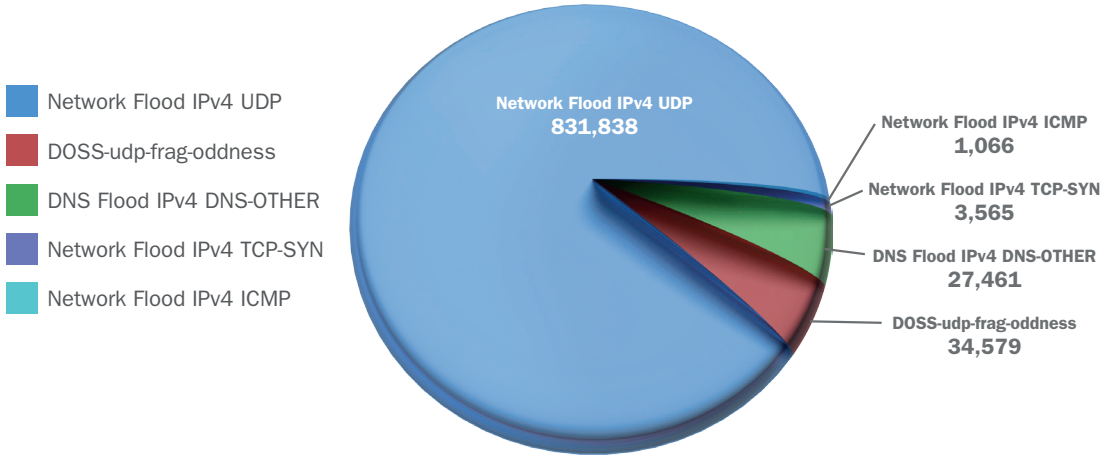
Known Attack Tool Name and Frequency



Most Prominent Attack Vectors

As seen in the following graph, the most prominent attack method by accumulated bandwidth was UDP flood, which is accountable for as much as ~ 800GB of traffic. More details regarding this attack can be found in this report.

Top Attacks by Bandwidth Consumption (Total MBytes)



Attacking Sources Geo-Location

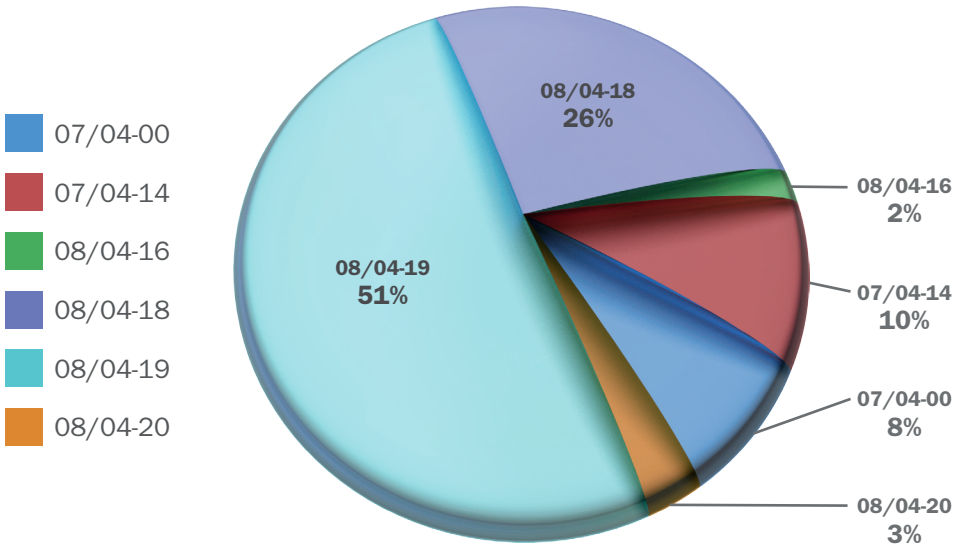
Geo-location tests the attacking IP addresses and shows a concentration of attackers originating in Europe.

Note that when looking at sources, two factors must be taken into consideration- some of the source IP addresses might have been spoofed or are part of a botnet.

Attack Peaks

Radware's Emergency Response Team (ERT) broke down the Denial-of-Service (DOS) attacks into significant times by bandwidth. The above average bandwidth of attacks were a percentage of the total bandwidth identified during the campaign. The results are indicated in the following graph which shows the main peaks of the campaign as a percentage of the total bandwidth identified by DP throughout the duration of the entire attack campaign.

Above Average Bandwidth Attacks as Percentage of the Total Bandwidth Identified During the Campaign



Attack Timetable

Date	Time (Israel Time)	% of Traffic[1]	Event
Sunday 07.04.13	~00:00	08%	Several UDP flood attacks were observed towards multiple destinations. Attack traffic reached ~ 65 GB. These attacks were accompanied by LOIC attacks (mostly LOIC/TCP), with emphasis on 3 specific targets.
Sunday 07.04.13	~14:00 ~18:00	10% 26%	Customers suffered from two waves of attacks, with more than 20% growth from the last big wave. At both times, attack traffic accumulated to more than ~ 77 GB. Alongside the UDP flood, two other vectors were added to the attack, high volume TCP-SYN floods and Fragmented ICMP floods. DNS Servers witnessed over 2 million malicious DNS queries over the passing hour.
Monday 08.04.13	~19:00	51%	The 3rd wave the customer has suffered was the biggest and most significant. UDP flood vector has amplified and reached a peak value of almost 400 GB of traffic. Attacks incorporated all vectors seen before, but in this specific wave, a slow connection attack was added to the list of attacks, mostly using the Slowloris attack tool. Slow HTTP vector targeted specific web hosting services.
Tuesday 09.04.13	~00:00 ~13:00	Low rate	The last day on record, included mainly LOIC, Slowloris and DNS Query floods.

[1] Amount of dropped traffic, out of all traffic measured during the time of the report on all DefensePro's.

Attack Details
Attack Vector 1: TCP-SYN Floods
Attack Description

DefensePro mitigated several TCP-SYN floods throughout the duration of the attack campaign, which varied in target and velocity. These attacks are aimed at consuming connection resources on the backend servers themselves and on stateful elements, like FW and load balancers, by sending numerous TCP-SYN requests toward targeted services while spoofing the attack packets source IP.

Date and Time	Target IP/Port	Mbps	KPPS
4/7/2013 6:38:21 PM	xx.xx.xxx.xxx/80	20	51
4/8/2013 11:56:45 AM	xx.xxx.xxx.xxx/80	10	30
4/8/2013 6:32:53 PM	xxx.x.xxx.xx/80	20	82
4/8/2013 6:59:29 PM	xx.xxx.xx.xx/80	2	5
4/8/2013 7:11:56 PM	xxx.x.xxx.xx/80	1.9	3.7
4/9/2013 1:58:49 PM	xx.xxx.xxx.xxx/80 xx.xxx.xxx.xxx/80	15	34
4/9/2013 3:01:14 PM	xx.xxx.xxx.xxx/80	6	14

Attack Potential Impact

- Exhaust resources of Firewall/IPS/etc.
- Exhaust resources of the web server

Attack Mitigation

Attacks were identified by DefensePro's behavioral protection which created an RT signature for the attack pattern.

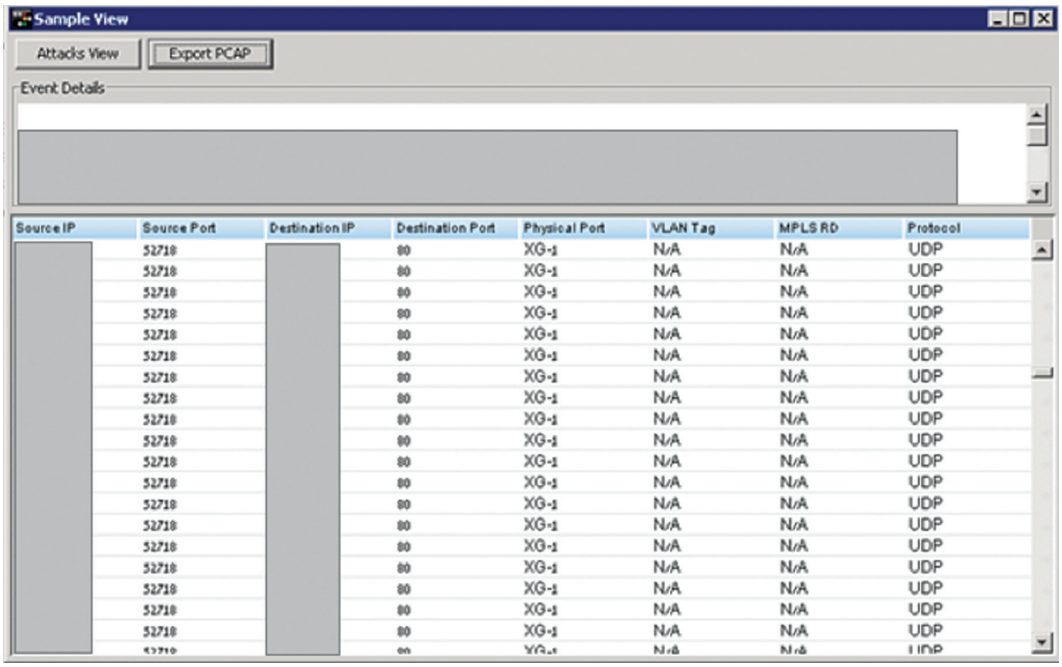
Attack Vector 2: UDP Floods

Attack Description

In a UDP flood one would try to saturate bandwidth in order to bring about a DoS state to the network. This is normally done by sending a rapid succession of UDP datagram's with spoofed IP addresses to a server within the network via various different ports. This will force the server to respond with ICMP traffic. The saturation of bandwidth happens both on the ingress and the egress direction.

In the following snapshot taken from the Vision Reporter, we can see a sample of one of the UDP floods that the customer suffered from.

The attacker uses an IP address, presumed to be spoofed (is related to a web hosting company in Amsterdam), while sending UDP packets to port 80:



Some of the traffic seen under the UDP Flood vector was fragmented UDP packets, stopped by the DoS shield mechanism. Network equipment such as routers and firewalls inspect fragmented packets in order to enforce RFC compliance by reassembling the packets into a valid 'flow'. Combining large amounts of fragmented UDP packets in a DoS attack, not only saturates bandwidth, but also creates a heavy load on the CPU of routers and firewalls in the path.

Attack Potential Impact

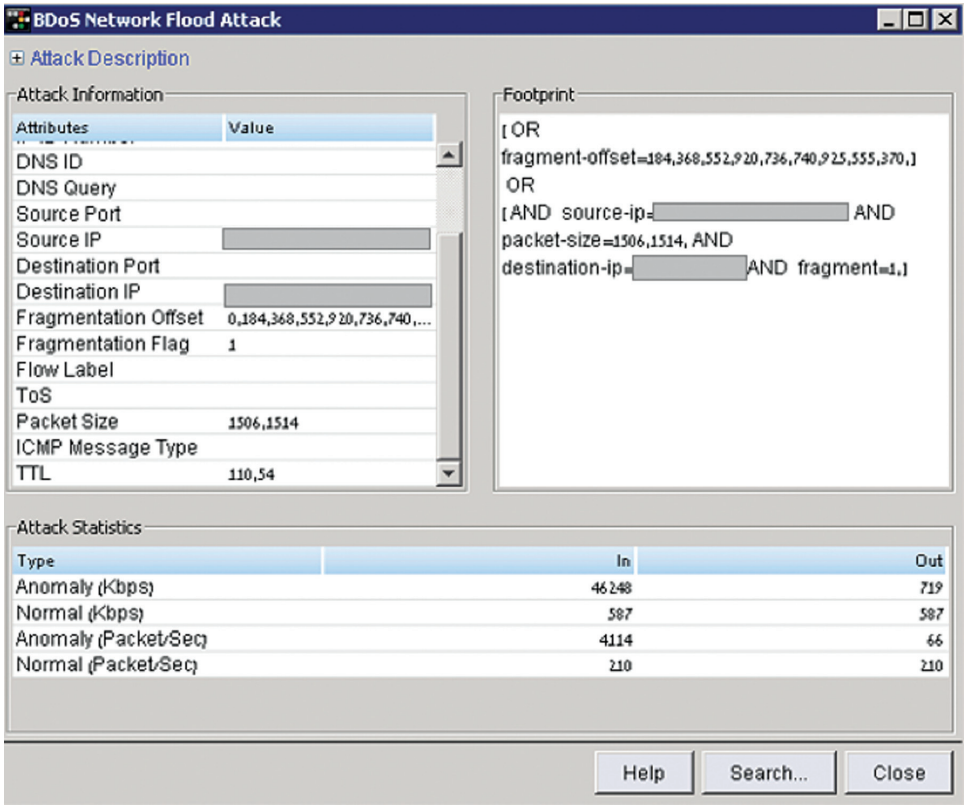
- Saturate bandwidth downstream using big UDP packets.
- Saturate bandwidth upstream and possibly tie up web servers processing resources for replying with ICMP destination unreachable packets.
- Create a heavy CPU load on other state full devices.

Attack Mitigation

BDOS

The DefensePro's behavioral DoS mechanism has reacted to the attacks by creating an RT signature for the attack vector.

As seen in the following screenshot, BDoS used specific parameters to create a footprint of the exact attack. In this case, a combination of **2 particular sizes** of packets which include **fragmented** flags set to and specific **TTLs**. Moreover, BDoS has identified that the normal rate of these types of packets is ~ 210 PPS, and at the attack time, there were ~ 4K PPS:



DoS Shield

DoS shield is one of the most bandwidth efficient mitigation mechanisms in DefensePro and is signature oriented. In this attack we could see the DoS shield had identified an abnormal increase in fragmented UDP packets and stopped them from crossing into the customer's premises.

The peak of this attack vector was on the morning of 09.04.13. At that time we witnessed as much as 11 different UDP attacks stopped by the DoS shield, with an average bandwidth of 23Mbps and some of the attacks lasting over 30 minutes.

Attack Vector 3: TCP-RST Floods

Attack Description

TCP reset flood can influence a server or a network in several ways. An RST flood could cause bandwidth saturation using massive amounts of traffic, could use up connections on a servers connection table (if no firewall is present in the path to check the state-fullness of the connection), and in the highly unlikely scenario that the RST packet was sent with the right ID and source, could kill a legitimate connection.

In the recent attack campaign, we witnessed a small amount of events using this vector.

Attack Potential Impact

- Bandwidth saturation
- Consume servers' connection table

Attack Mitigation

This type of attack was mitigated in DefensePro by BDoS which creates a RT signature of the attack and blocks all related traffic.

Attack Vector 4: DNS Floods

Attack Description

Several high-rate DNS Query floods targeted the environment throughout the attack campaign, which amounted to up to 66Mbps, 101K PPS. In a DNS flood, the attacker bombards the targeted DNS servers with DNS queries while spoofing the source IPs, forcing the server to send numerous responses to non-existing clients. DNS floods targeting the network comprise mainly of DNS queries for 'ANY' or 'A' records registered on various domains. By sending queries for 'ANY' record type associated with a specific domain, attackers were able to leverage the asymmetric nature of the DNS protocol and create an amplified attack - while the original query was probably under 100 bytes long, the response for 'ANY' record can amount to several thousand bytes, consuming outbound bandwidth.

Start Time	Mbps	KPPS	Total Minutes
4/6/2013 23:17	2.24	3.42	12.58
4/7/2013 23:41	2.19	3.28	5.12
4/8/2013 1:58	2.24	3.23	15.23
4/8/2013 7:52	2.07	2.99	3.25
4/8/2013 21:30	2.02	3.09	4.15
4/8/2013 23:09	6.51	9.91	77.4
4/8/2013 23:10	2.09	3.19	77.2
4/9/2013 13:22	2.4	3.56	17.27

Attack Potential Impact

- Inbound bandwidth consumption by the query flood itself
- Outbound bandwidth saturation by forcing the DNS server to send oversized DNS responses
- DNS server denial of service
- Paralyze the network by hitting the DNS infrastructure

Attack Mitigation

All DNS attacks were identified and mitigated using DNS protection, a protection mechanism which recognizes deviations in traffic rate and distribution, and enforces various mitigation techniques once an attack is detected. These include real time signature creation and applying DNS challenges on DNS traffic.

Attack Vector 5: ICMP Floods

Attack Description

Multiple hosts were targeted with various ICMP floods, many of these comprised of fragmented ICMP traffic. Apart from bandwidth consumption, ICMP floods can also impact firewalls of targeted networks which treat ICMP messages. By fragmenting the attack packets, attackers add another layer of complexity for targeted equipment.

Time	Fragmented	Target	Mbps	KPPS
4/6/2013 1:40	Non fragmented	Multiple	4.79	5.45
4/7/2013 1:45	Non fragmented	Multiple	3.62	4.15
4/7/2013 14:48	Fragmented	xx.xxx.xxx.xxx	2.38	0.22
4/7/2013 20:04 ~ 4/7/2013 23:16	Fragmented	xxx.x.xx.xx xx.xxx.xx.xx	Up to 50.02	Up to 4.22
4/8/2013 18:33	Non fragmented	Multiple	2.84	4.64
4/8/2013 21:57 ~ 4/8/2013 23:07	Fragmented	xx.xxx.xx.xx	Up to 9.9	Up to 0.8
4/9/2013 1:46	Fragmented	xx.xx.xx.xx	10.81	0.91

Attack Potential Impact

- Saturate bandwidth upstream
- Consume firewall resources

Attack Mitigation

BDOS

In several occasions BDoS identified an abnormal increase of inbound ICMP traffic. Once triggered, BDoS was able to build an RT signature for attack traffic and mitigate the attacks.

DoS Shield

A static signature applied on DP is intended to identify abnormal high-rates of fragmented ICMP traffic. Once triggered, this signature applies strict fragmented ICMP rate limit on DefensePro HW accelerator.

Attack Vector 6: LOIC

Attack Description

LOIC is a windows based attack tool capable of generating TCP/UDP data floods and HTTP requests floods. Using various versions of the LOIC attack tool, attackers sent multiple TCP/UDP data packets with constant payload towards TPC/80 on the targeted web servers. DefensePro identified and blocked this attack vector using several IPS signatures.

For more information on LOIC, see http://security.radware.com/knowledge-center/DDoSPedia/loic-low-orbit-ion-cannon/

Attack Potential Impact

- UDP attack vector will mainly consume targeted network bandwidth
- TCP attack vector fills targeted server's connection resources

Attack Mitigation

This attack tools was identified and blocked using 7 IPS signatures:

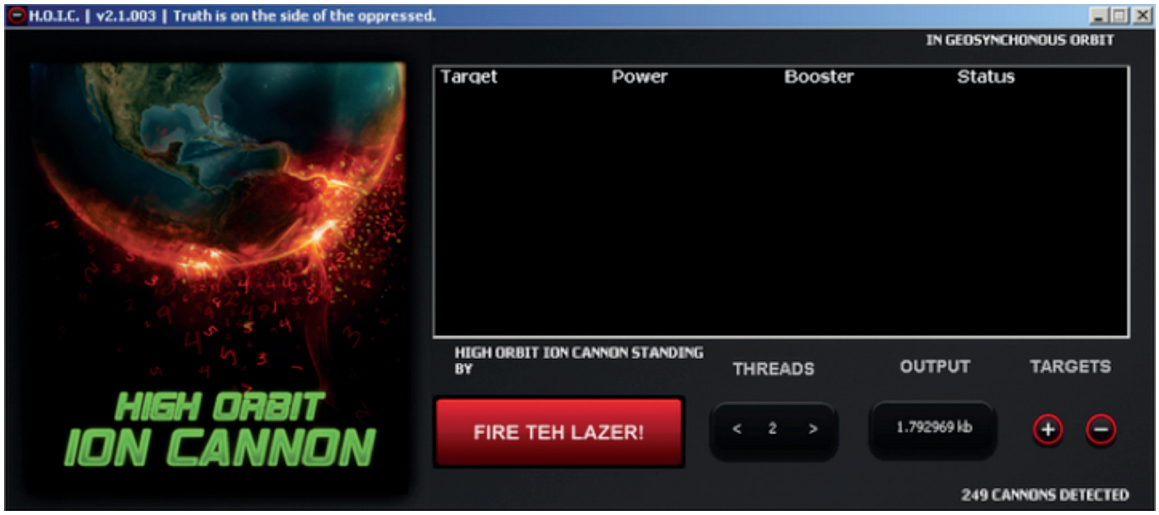
Signature ID	Signature Name
13926	DOS-LOIC-UDP-80-cat
13928	DOS-LOIC-TCP-80-cat
13916	DOS-LOIC-TCP-80-dun
14972	DOS-LOIC-TCP-80-revolucion
13922	DOS-LOIC-UDP-80-dun
14976	DOS-LOIC-UDP-80-revolucion

Attack Vector 7: HOIC

Attack Description

HOIC (High Orbit Cannon Laser) is a Windows based DoS attack tool used for generating HTTP floods. It's capable of flooding the targeted host with multiple HTTP requests while randomizing various HTTP header fields in order to evade IPS systems.

For more information on HOIC, visit: http://security.radware.com/knowledge-center/DDoSPedia/hoic-high-orbit-ion-cannon/



Attack Potential Impact

- Exhaust web server resources

Attack Mitigation

HOIC was identified and blocked by a DefensePro IPS signature RWID 15840.

Attack Vector 8: Slowloris Attack

Attack Description

Slowloris is a slow HTTP DoS tool sending incomplete HTTP requests. It sends one CRLF at the end of the HTTP request header instead of two, which causes a time out to the web server and leaves more than one process running. This attack is implemented with very little computing resources on the attacker's side.

For more information on Slowloris, see http://security.radware.com/slowloris/

Attack Potential Impact

Complete DoS of targeted web server.

Attack Mitigation

Slowloris was identified and blocked using an IPS signature RWID 10526.

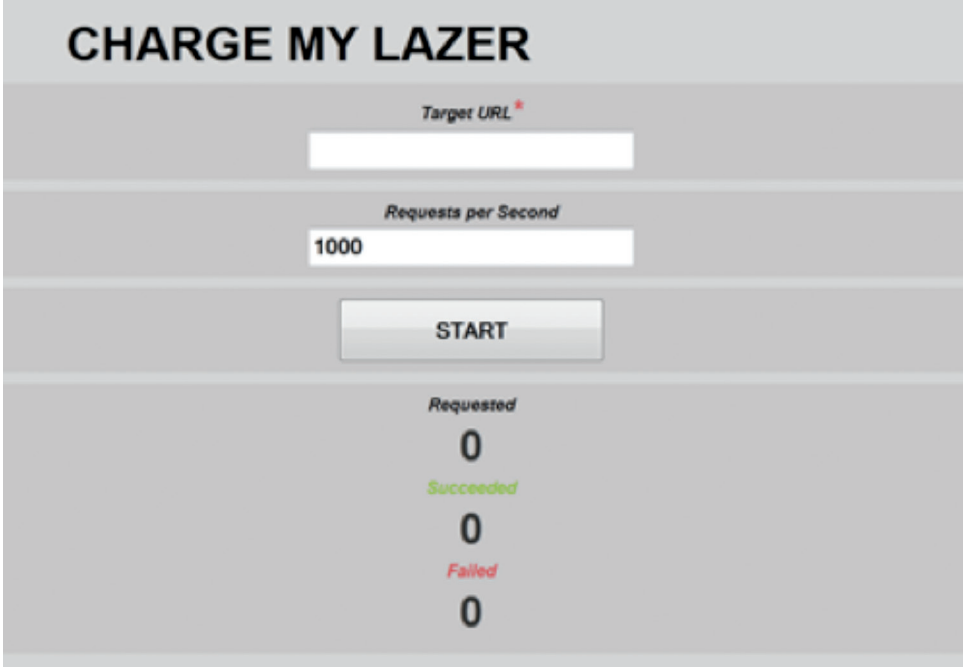
Attack Vector 9: Apache Killer

Attack Description

"Apache Killer" tool exploits a severe vulnerability in the widely used Apache web server (CVE-2011-3192). The tool sends a large number of overlapping "byte ranges" HTTP requests to an Apache server, effectively causing the server to run out of useable memory. Anonymous has created a web GUI version of this tool, referred to as 'Mobile LOIC Apache Killer', which allows their followers to easily leverage this attack.

Based on reports generated by DefensePro, we can confirm both the script version of the tool ('Apache Killer') and the web GUI version ('Mobile LOIC') were used by attackers.

For more information on Apache Killer see: http://security.radware.com/knowledge-center/DDoSPedia/Apache-Killer/



Attack Potential Impact
Exploitation of this attack tool against vulnerable Apache web servers may lead to complete DoS.

Attack Mitigation
This attack tool was identified and mitigated using two DP IPS signatures: RWID 15074 and RWID 15416.