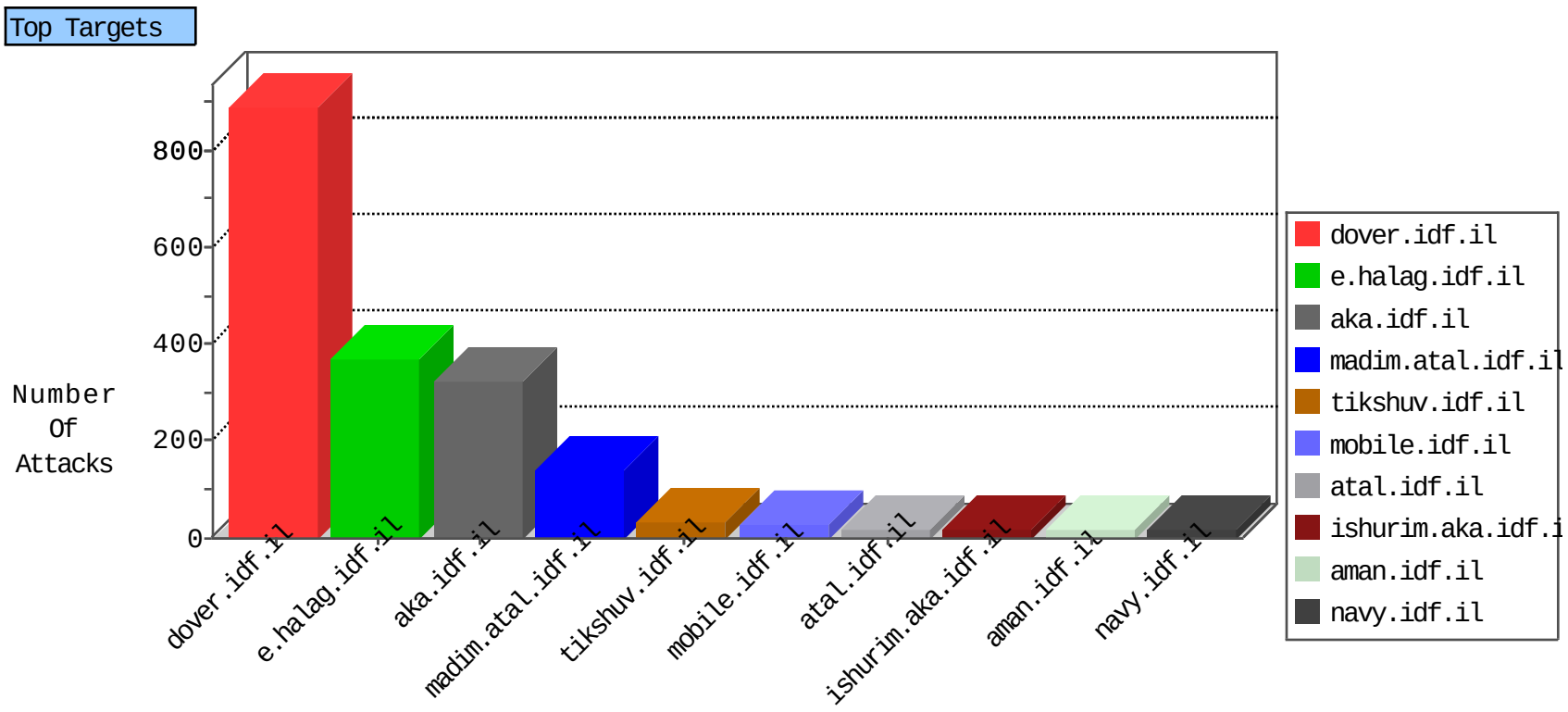
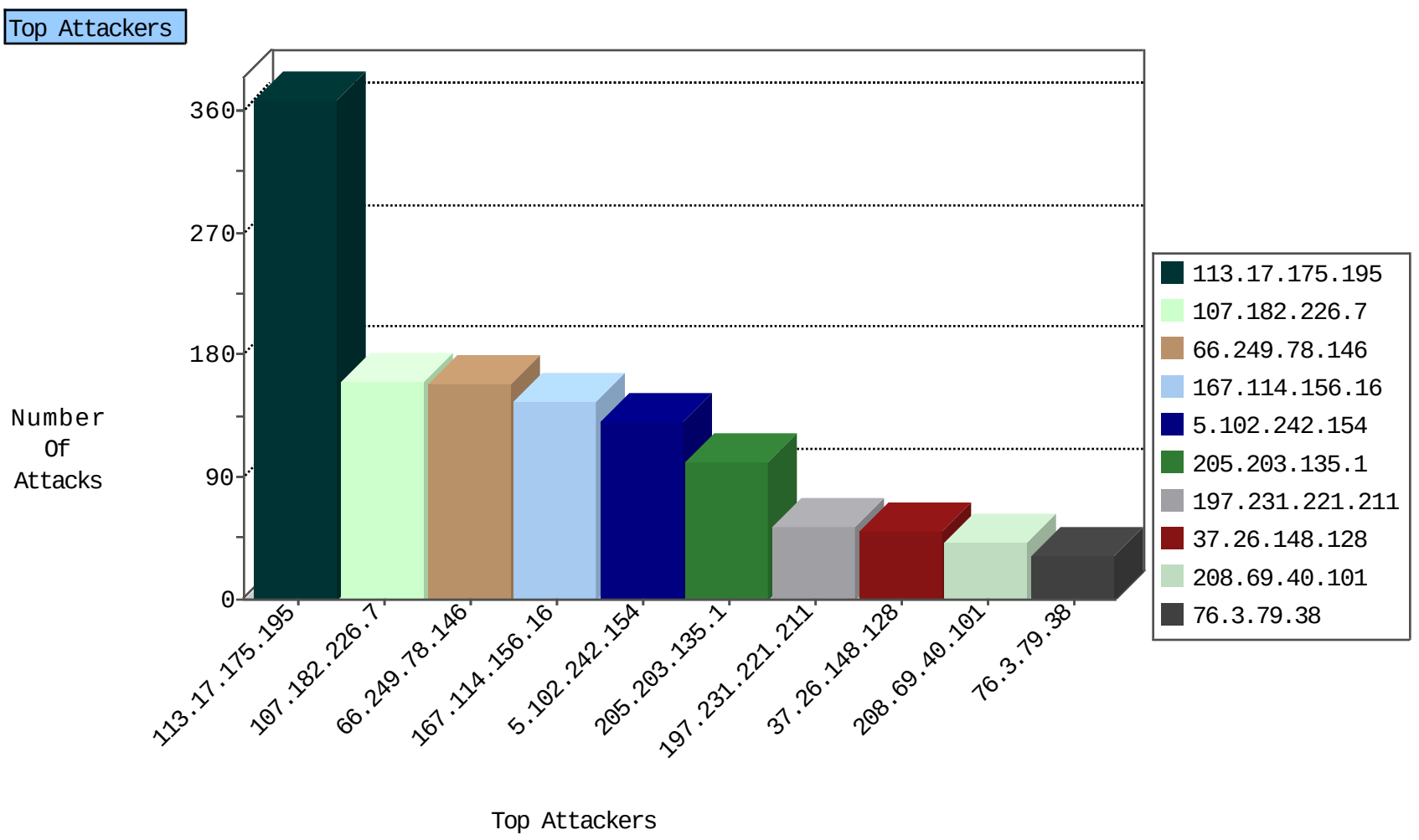
04-24-2016-22:04:03 to 04-24-2016-23:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-24-2016-22:04:03 to 04-24-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7456
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	368
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	368
46.19.86.223	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
69.197.185.20	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
91.183.186.227	Belgium	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
74.91.17.181	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
74.91.18.42	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
173.208.197.251	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
74.91.17.180	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
124.232.150.230	China	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
74.91.18.43	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
69.30.198.150	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
74.91.23.110	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
69.197.185.20	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
107.150.32.60	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
74.91.17.182	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1

04-24-2016-22:04:03 to 04-24-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

04-24-2016-22:04:03 to 04-24-2016-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4

04-24-2016-22:04:03 to 04-24-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.182.226.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	161
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	159
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
37.26.148.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
76.3.79.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
5.22.129.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
141.0.15.154	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.181.136.108	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.125.114.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
190.236.54.210	Peru	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.65.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.253.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.184.70.225	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.166.34	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.124.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.212.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
174.57.63.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.182	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.11.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.207.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.54.163.3	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
95.185.217.220	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
52.71.155.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.145.220.87	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.159.168.35	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
134.35.238.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
95.185.217.220	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
95.185.217.220	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.54.163.3	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
40.77.167.43	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.242.154	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	128
213.8.204.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.29	Block	11
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
87.69.62.195	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.69.62.195 (Open Mode)	None	3
5.102.242.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.23.191	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 149.78.23.191	Block	2
149.78.23.191	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	2
141.212.122.129	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /x	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
164.132.161.41	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
87.69.62.195	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
74.91.17.180	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.xy966.com/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
94.159.153.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.78.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
213.8.204.29	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
40.77.167.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
74.91.23.110	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.178tx.com/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
109.67.29.221	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sachar/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/eitan/listpage/	Block	1
46.19.86.229	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
149.78.23.191	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
85.65.98.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluim/templates/www.behazdaa.org.il	Block	1
188.228.98.138	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
2.53.169.70	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
134.35.238.238	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.79.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1
46.116.242.90	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
149.78.23.191	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/xmlrpc.php	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1