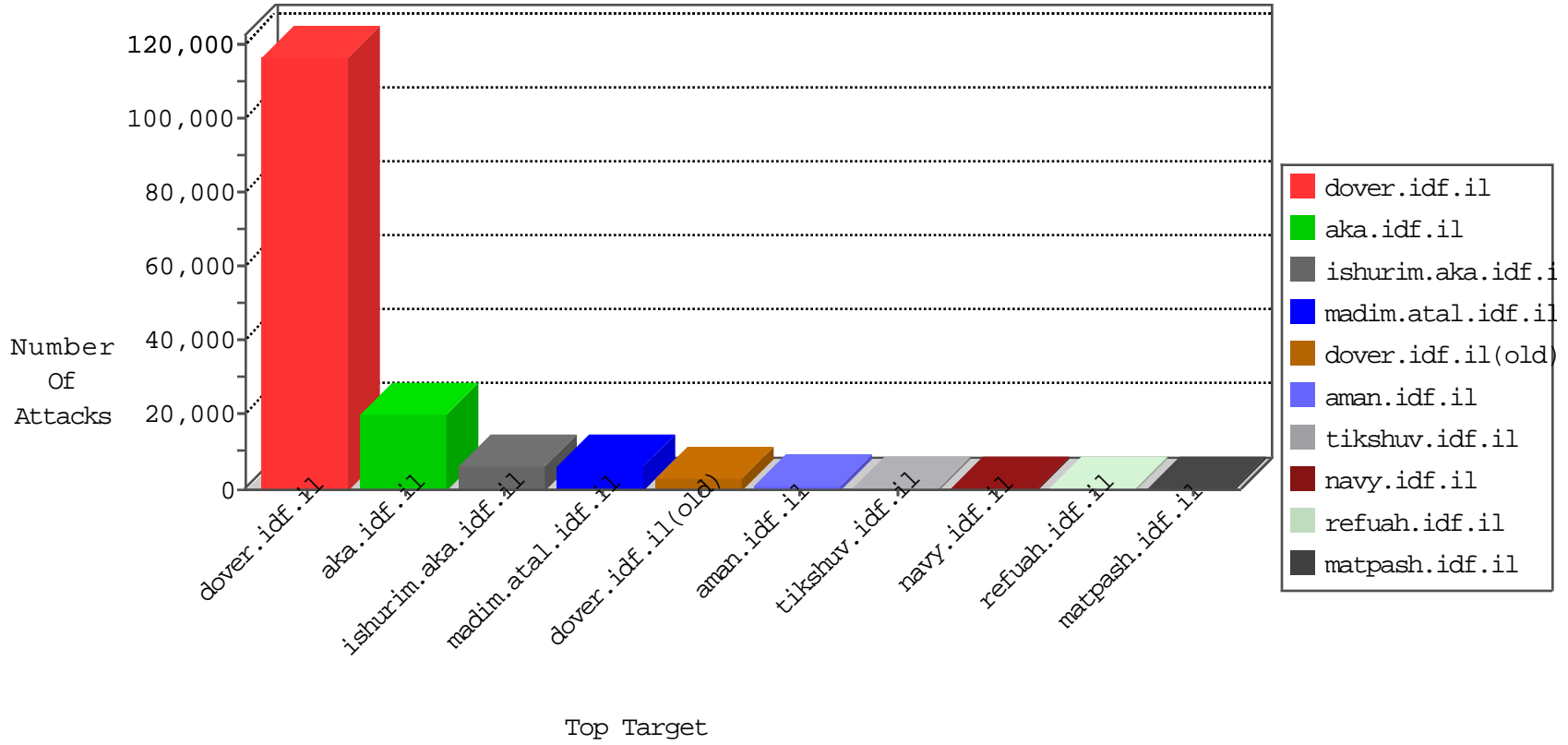


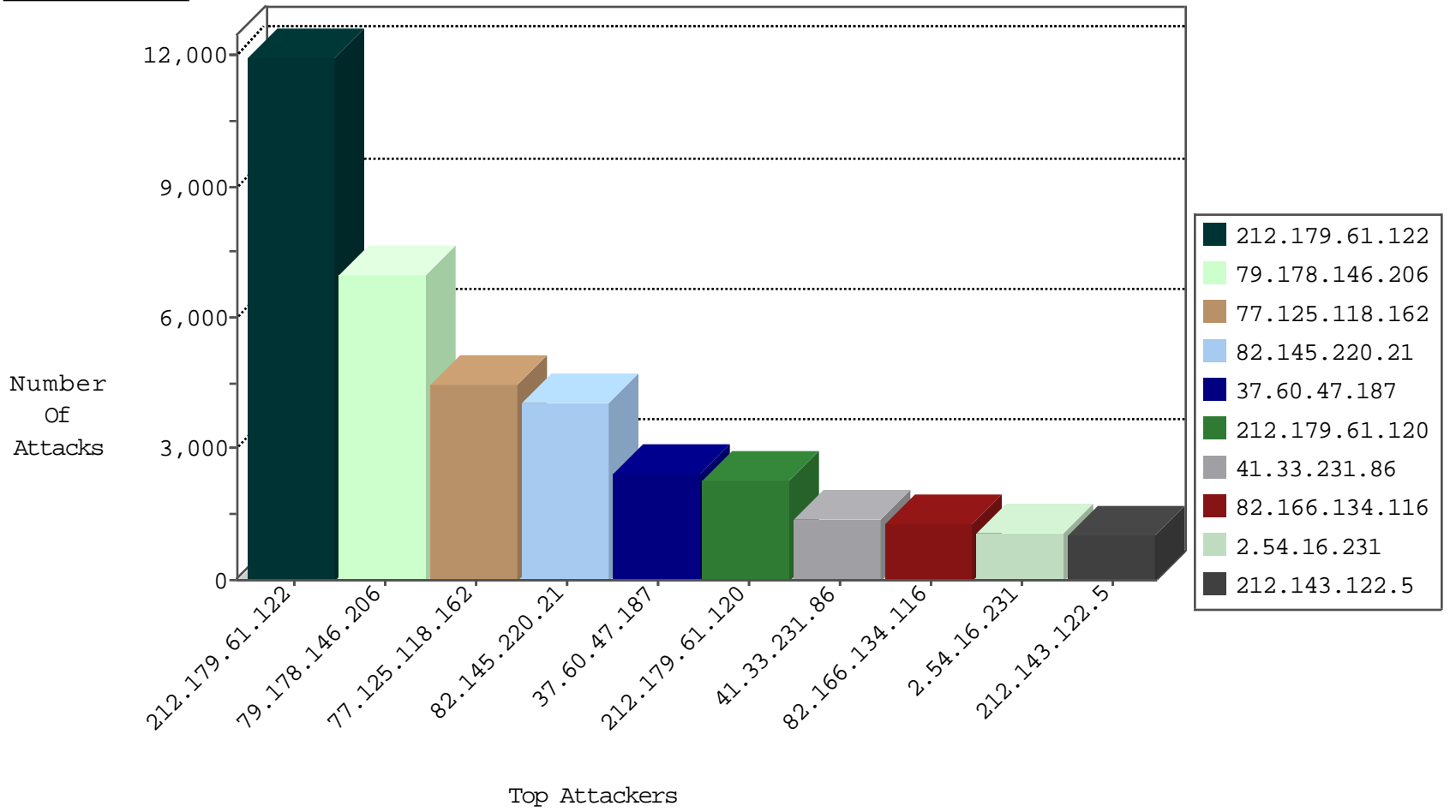
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.101	United States	147.237.72.14	dover.idf.il(ol	TCP handshake violation, first packet not syn	drop	38997
66.249.78.115	United States	147.237.72.14	dover.idf.il(ol	TCP handshake violation, first packet not syn	drop	24940
66.249.78.158	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21561
66.249.78.172	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18549
66.249.64.45	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	13828
66.249.67.31	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	11341
82.205.63.243	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11235
82.205.63.233	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8994
66.249.64.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8120
66.249.78.108	United States	147.237.72.14	dover.idf.il(ol	TCP handshake violation, first packet not syn	drop	8101
82.205.97.222	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7793
82.205.51.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7172
74.95.205.129	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5816
66.249.64.116	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5656
212.106.68.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5492
66.249.64.37	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5122
212.106.76.49	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4983
109.154.151.40	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4705
66.249.64.124	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4305
174.112.46.146	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3954
212.106.65.237	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3906
212.106.87.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3849
77.102.192.69	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3408
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3303
212.106.79.102	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3277
212.227.134.90	Germany	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3234
37.8.117.151	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3102
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3072
212.179.61.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2973
24.46.153.202	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2863
212.179.61.122	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2740
92.115.181.39	Moldova, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2651
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2510
216.244.22.239	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2305
82.205.109.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2275
66.249.78.189	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2256
82.102.204.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2009
217.66.247.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1628
66.249.78.165	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1602
65.19.138.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1532
85.113.106.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1414
208.115.111.70	United States	147.237.72.14	dover.idf.il(ol	TCP handshake violation, first packet not syn	drop	1342
66.249.64.168	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1302
66.249.67.23	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1212
87.61.240.106	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1126
82.102.199.23	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1124
77.221.140.163	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1117

11-16-2014-00:00:05 to 11-17-2014-00:00:05

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
82.205.59.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1093
207.46.13.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1092
186.207.131.108	Brazil	147.237.72.14	dover.idf.il(olc	TCP handshake violation, first packet not syn	drop	1083

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.228.185.157	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	25
109.66.48.8	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
37.230.14.221	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.57.223.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
77.125.89.81	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.66.172.109	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.177.174.180	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
184.152.58.142	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
87.68.19.79	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
80.74.111.178	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
106.138.33.144	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.67.163.233	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
113.87.53.145	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
79.180.162.188	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.117.214.253	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.152.3.173	Germany	147.237.72.166	aka.idf.il	1106: HTTP: IIS .%.5c Encoded \ in URI	Permit	4
212.235.20.125	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.24	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.225.59	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.64.152.63	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.245.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.125	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.21	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
149.78.27.33	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.86.16	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.167.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
2.54.187.114	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.179.129.145	Germany	147.237.77.216	dover.idf.il	Block_Level_70_100	Block	3
89.139.89.167	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.66.140.212	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.108.219.232	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.136.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
94.159.158.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.181.63.83	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.172.48.0	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.28.145.141	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.80.17.163	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
87.69.36.237	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
129.119.5.221	United States	147.237.72.14	dover.idf.il(old)	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.205.51.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	2
46.19.85.117	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.64.143.55	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
2.54.136.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.137.88	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.78.115.70	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
94.159.221.196	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
192.116.96.186	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
87.69.146.240	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.110.86.187	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.229.41	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	168
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	82
2.54.21.59	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
93.172.170.50	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
109.66.165.242	Israel	147.237.77.170	maarachot.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	4
37.142.101.245	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
37.142.123.181	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.64.51.207	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.64.25	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
79.177.193.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
96.45.180.58	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
96.45.180.58	Canada	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
84.228.106.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.121.137.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.27.205	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
178.33.253.101	France	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
79.176.17.22	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.135.102.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
178.62.78.61	Netherlands	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
37.26.147.137	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.109.235.122	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
77.125.166.105	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.182.142.85	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.249.16	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.238.61	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.182.197	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.201.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.156.90	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.8.223	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.251.64	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.102.141.213	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
96.45.180.58	Canada	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
128.103.64.112	United States	147.237.72.14	dover.idf.il(old)	Tehila - Perl LWP with fake user agent	2
199.167.41.202	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
79.176.194.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.112.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.46.158	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.74.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.18.185	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.73.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.216	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
71.169.2.90	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
213.57.216.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.161.87	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.91.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.161.234	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.87.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
203.156.118.25	Thailand	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
89.139.73.195	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.122	Israel	147.237.77.216	dover.idf.il		drop	drop	11948
79.178.146.206	Israel	147.237.77.216	dover.idf.il		drop	drop	6977
77.125.118.162	Israel	147.237.77.216	dover.idf.il		drop	drop	4467
82.145.220.21	Europe	147.237.77.216	dover.idf.il		drop	drop	4014
37.60.47.187	Israel	147.237.77.216	dover.idf.il		drop	drop	2442
212.179.61.120	Israel	147.237.77.216	dover.idf.il		drop	drop	2255
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1364
82.166.134.116	Israel	147.237.77.216	dover.idf.il		drop	drop	1305
2.54.16.231	Israel	147.237.77.216	dover.idf.il		drop	drop	1088
212.143.122.5	Israel	147.237.77.216	dover.idf.il		drop	drop	998
212.179.61.124	Israel	147.237.77.216	dover.idf.il		drop	drop	924
208.115.113.89	United States	147.237.77.216	dover.idf.il		drop	drop	858
31.44.135.4	Israel	147.237.77.216	dover.idf.il		drop	drop	756
5.28.131.214	Israel	147.237.77.216	dover.idf.il		drop	drop	733
208.115.111.73	United States	147.237.77.216	dover.idf.il		drop	drop	711
46.117.127.30	Israel	147.237.77.216	dover.idf.il		drop	drop	684
37.26.147.182	Israel	147.237.77.216	dover.idf.il		drop	drop	654
54.72.0.55	United States	147.237.77.216	dover.idf.il		drop	drop	652
54.72.73.168	United States	147.237.77.216	dover.idf.il		drop	drop	624
109.66.148.53	Israel	147.237.77.216	dover.idf.il		drop	drop	623
46.19.85.24	Israel	147.237.77.216	dover.idf.il		drop	drop	589
212.179.21.194	Israel	147.237.77.216	dover.idf.il		drop	drop	579
2.54.160.7	Israel	147.237.77.216	dover.idf.il		drop	drop	563
149.88.81.185	United States	147.237.77.216	dover.idf.il		drop	drop	562
66.249.78.172	United States	147.237.77.216	dover.idf.il		drop	drop	557
2.54.29.182	Israel	147.237.77.216	dover.idf.il		drop	drop	546
37.60.44.50	Israel	147.237.77.216	dover.idf.il		drop	drop	541
68.180.228.121	United States	147.237.77.216	dover.idf.il		drop	drop	496
82.166.3.72	Israel	147.237.77.216	dover.idf.il		drop	drop	496
66.249.78.158	United States	147.237.77.216	dover.idf.il		drop	drop	495
212.179.21.196	Israel	147.237.77.216	dover.idf.il		drop	drop	493
212.179.61.126	Israel	147.237.77.216	dover.idf.il		drop	drop	490
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	463
92.243.196.73	Czech Republic	147.237.77.216	dover.idf.il		drop	drop	452
46.19.85.30	Israel	147.237.77.216	dover.idf.il		drop	drop	438
192.115.189.20	Israel	147.237.77.216	dover.idf.il		drop	drop	433
71.89.73.143	United States	147.237.77.216	dover.idf.il		drop	drop	415
50.87.144.145	United States	147.237.77.216	dover.idf.il		drop	drop	412
212.76.124.118	Israel	147.237.77.216	dover.idf.il		drop	drop	410
46.121.247.94	Israel	147.237.77.216	dover.idf.il		drop	drop	408
79.183.49.49	Israel	147.237.77.216	dover.idf.il		drop	drop	360
149.78.51.199	Israel	147.237.77.216	dover.idf.il		drop	drop	355
37.26.146.181	Israel	147.237.77.216	dover.idf.il		drop	drop	335
37.142.143.198	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	319
195.34.150.18	Austria	147.237.77.216	dover.idf.il		drop	drop	315
201.227.105.108	Panama	147.237.77.216	dover.idf.il		drop	drop	304
46.19.85.37	Israel	147.237.77.216	dover.idf.il		drop	drop	292
89.138.222.185	Israel	147.237.77.216	dover.idf.il		drop	drop	288
93.172.167.188	Israel	147.237.77.216	dover.idf.il		drop	drop	288
2.54.19.187	Israel	147.237.77.216	dover.idf.il		drop	drop	284

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.66.9.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	500
46.117.157.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	419
109.66.165.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	379
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	355
2.54.158.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	295
109.253.80.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	284
109.253.157.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	277
109.253.158.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	273
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	264
176.12.144.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	216
10.110.110.38		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	209
5.29.201.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	206
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	192
80.246.139.58	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.139.58	Block	151
176.12.138.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	137
176.12.144.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	131
109.253.138.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	130
176.12.137.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	125
84.108.80.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	125
37.26.147.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	124
109.253.134.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	123
109.253.145.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	122
176.12.149.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
109.253.140.138	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.140.138	Block	102
66.249.64.120	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.120	Block	99
66.249.64.116	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.116	Block	96
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
62.219.13.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	91
46.210.134.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
109.253.123.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	83
79.176.163.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
2.54.22.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
209.95.34.86	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	71
213.57.214.41	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Suspicious Response Code	Block	69
66.249.64.124	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.124	Block	67
164.138.119.159	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	67
157.55.39.135	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	61
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
2.54.20.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	56
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	53
157.55.39.123	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	50
2.54.18.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	49
176.12.144.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	46
79.177.9.165	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.9.165	Block	46
77.126.229.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	45
77.126.41.23	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Suspicious Response Code	Block	45
85.64.228.146	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Suspicious Response Code	Block	45
84.228.185.157	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.228.185.157	Block	44