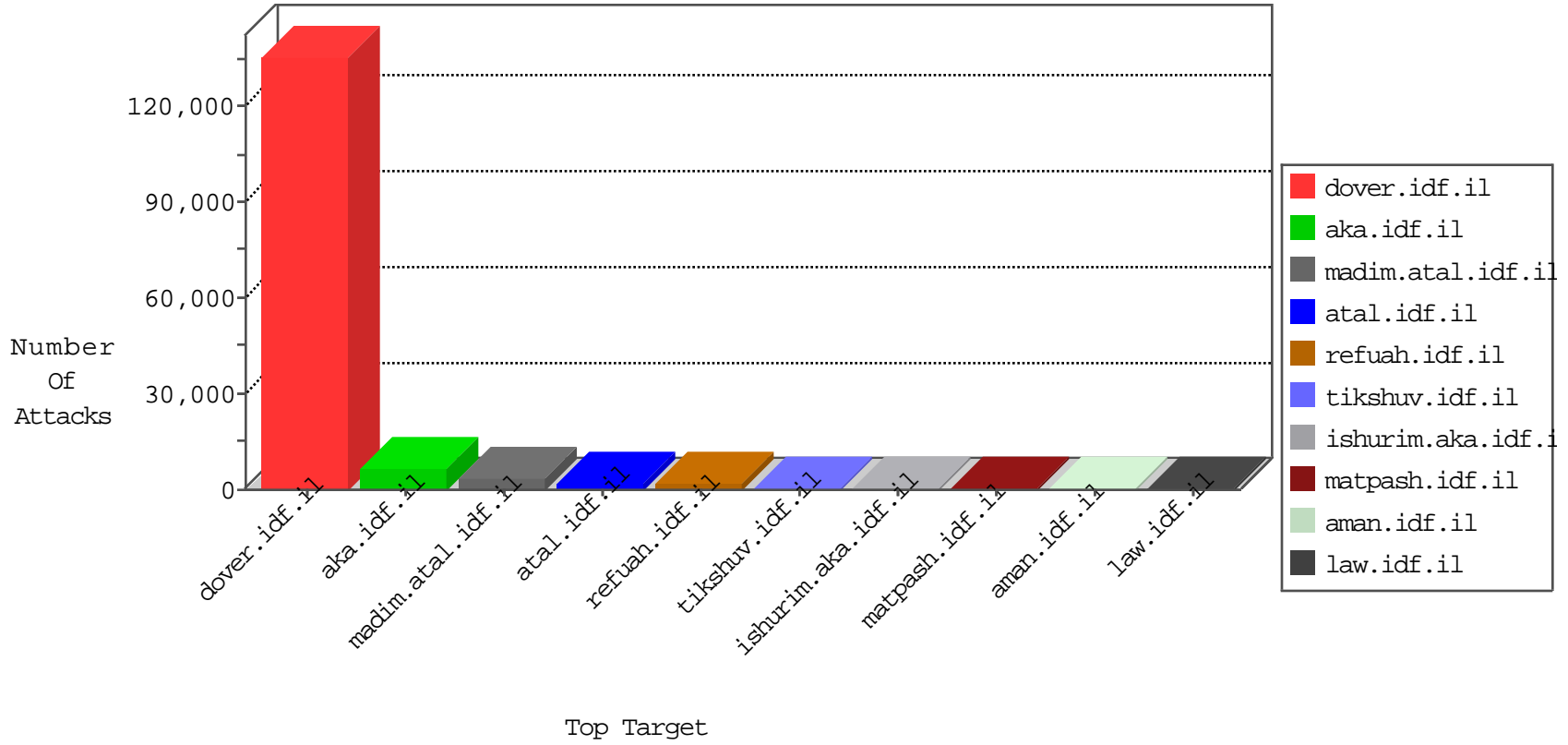


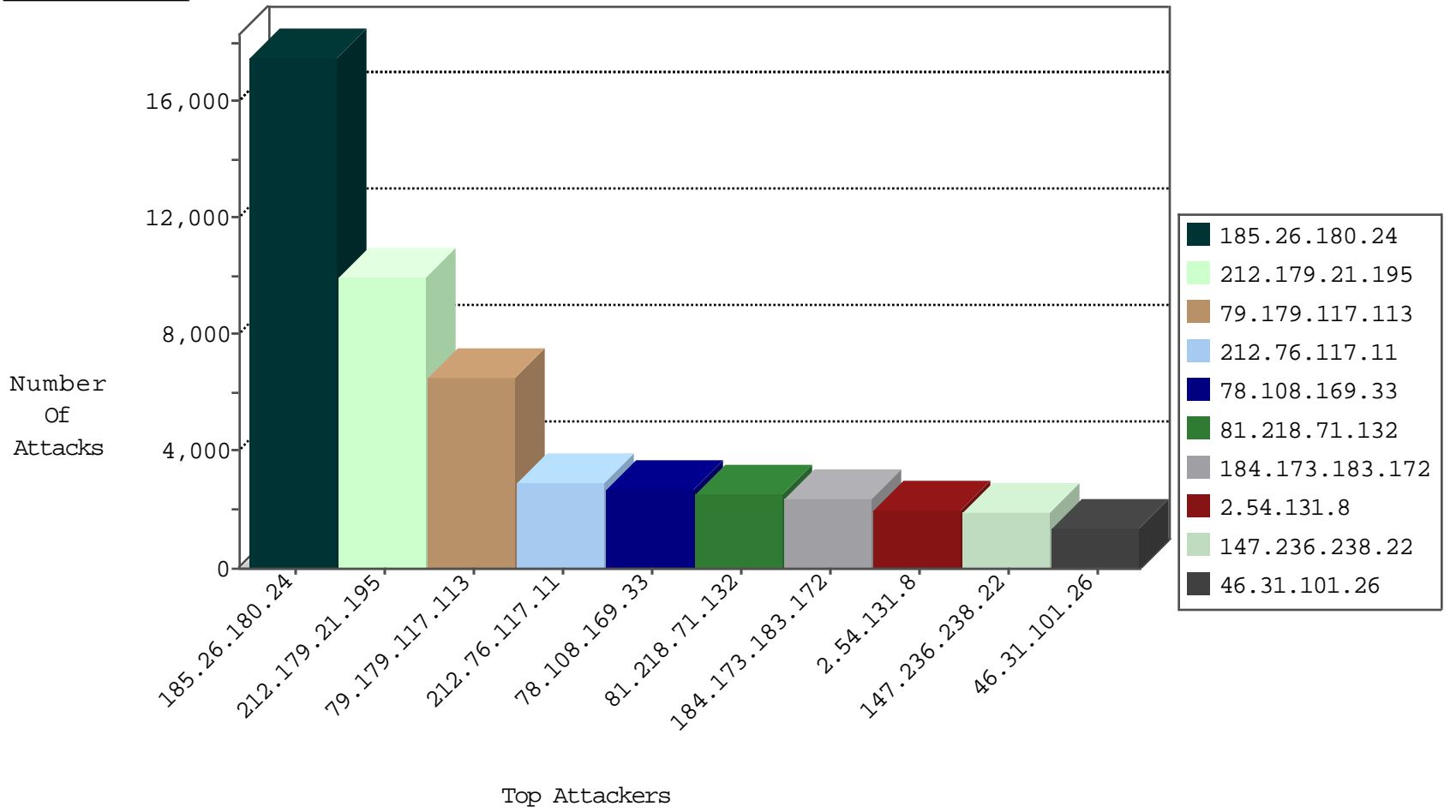
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.108	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7064
5.22.129.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6025
66.249.75.44	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	6019
84.109.125.229	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5981
190.242.83.23	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5943
212.179.21.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5681
185.26.180.24	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4066
220.181.108.122	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3998
220.181.108.104	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3879
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2872
212.199.38.133	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2651
66.249.67.116	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1951
66.249.67.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1396
66.249.67.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1126
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	976
79.178.178.165	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	494
85.65.144.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	419
109.64.2.103	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	412
220.181.108.90	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	398
84.228.155.215	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	379
220.181.108.175	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	330
220.181.108.184	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	313
46.19.85.124	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	295
220.181.108.169	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	253
84.228.250.40	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	248
84.111.65.42	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	229
220.181.108.146	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	204
31.168.84.241	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
79.177.34.220	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	188
109.253.135.151	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
46.116.154.68	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
79.179.60.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
94.159.195.214	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
93.172.27.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	150
77.125.72.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	141
213.151.51.175	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
5.102.214.119	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
220.181.108.111	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	118
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	118
46.116.180.190	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	116
77.127.233.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
176.12.151.230	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	103
220.181.108.156	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	103
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	99
66.249.67.100	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	88
109.253.142.172	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
85.250.59.118	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	1128
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	591
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	488
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	142
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	106
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	66
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	60
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	39
117.131.78.26	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	25
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
112.111.191.133	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
79.182.51.117	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
212.143.43.173	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	8
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	6
85.17.242.234	Netherlands	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
91.135.111.85	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	6
50.57.157.221	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	6
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
212.235.13.12	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
149.78.94.147	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.16	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
41.185.12.165	South Africa	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	5
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	5
84.111.30.39	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
122.2.21.141	Philippines	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
114.32.178.177	Taiwan	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
85.25.103.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	100
2.54.43.11	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	29
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	26
80.246.140.245	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	20
66.249.67.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	10
184.168.193.116	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	10
80.246.140.176	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	9
5.101.157.38	Russian Federation	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.116	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
178.19.107.114	Poland	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	3
79.176.102.36	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.46.193.114	China	147.237.77.234	halag.idf.il	GPL SCAN nmap TCP	2
91.224.132.118	Russian Federation	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.108	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.137.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
216.230.231.82	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
46.117.204.117	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.76.115.158	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.183.128.6	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
91.238.134.92	Poland	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.78	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
46.117.128.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
218.24.171.223	China	147.237.77.234	halag.idf.il	GPL SCAN nmap TCP	2
66.249.93.175	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
109.65.185.210	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.150.189.2	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.184.0	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.249.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.142	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.163	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
79.178.140.123	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
77.126.234.91	Israel	147.237.77.74	law.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
80.246.130.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
164.215.110.1	United States	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	2
2.52.14.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.98.152	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
80.178.158.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.147	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
89.221.250.4	Sweden	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
94.159.207.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.24	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17505
212.179.21.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9938
79.179.117.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6478
212.76.117.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2911
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2671
81.218.71.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2550
2.54.131.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2035
147.236.238.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1950
46.31.101.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1379
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1265
46.116.251.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1247
95.86.113.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1083
213.57.51.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	830
46.19.85.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	785
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	745
46.19.86.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	744
193.246.96.102	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	712
79.183.136.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	555
77.125.160.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	533
46.19.85.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	526
80.246.133.86	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	505
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	451
84.108.171.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	436
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	425
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	402
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	396
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	388
212.199.57.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	375
149.88.1.181	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	361
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	360
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	339
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	335
176.12.138.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	335
132.74.1.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	324
207.46.13.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	319
62.0.60.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	314
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	310
157.55.39.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	309
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	303
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	286
46.19.86.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	285
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	275
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	270
2.54.43.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	269
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
137.37.228.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
157.55.39.176	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	258
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	255
70.138.146.134	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	253
212.179.21.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
31.168.126.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	518
85.250.59.118	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.250.59.118	Block	389
94.159.172.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	288
31.168.170.54	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.168.170.54	Block	267
46.210.203.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	224
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 213.151.32.163	Block	220
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	179
31.168.170.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
109.253.158.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	158
2.54.143.114	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.143.114	Block	140
82.102.141.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	126
176.12.147.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	112
80.246.141.219	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.141.219	Block	93
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	88
207.46.13.43	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.43	Block	82
109.253.131.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	79
2.54.1.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	73
207.46.13.114	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.114	Block	66
79.176.220.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	54
2.52.8.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	47
207.46.13.50	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.50	Block	47
2.54.11.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
157.55.39.247	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.247	Block	40
176.12.142.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	36
207.232.55.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	33
176.12.143.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	32
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	29
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	29
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	27
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	27
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	26
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
207.46.13.114	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	22
62.90.131.34	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.90.131.34	Block	22
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	22
81.218.33.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	20
109.253.132.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
192.38.121.229	Denmark	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	18
91.224.27.230	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.224.27.230	Block	17
95.86.95.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	17
109.253.129.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15
213.151.53.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	14
176.12.137.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
213.151.47.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	14
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	14
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
157.55.39.179	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	12