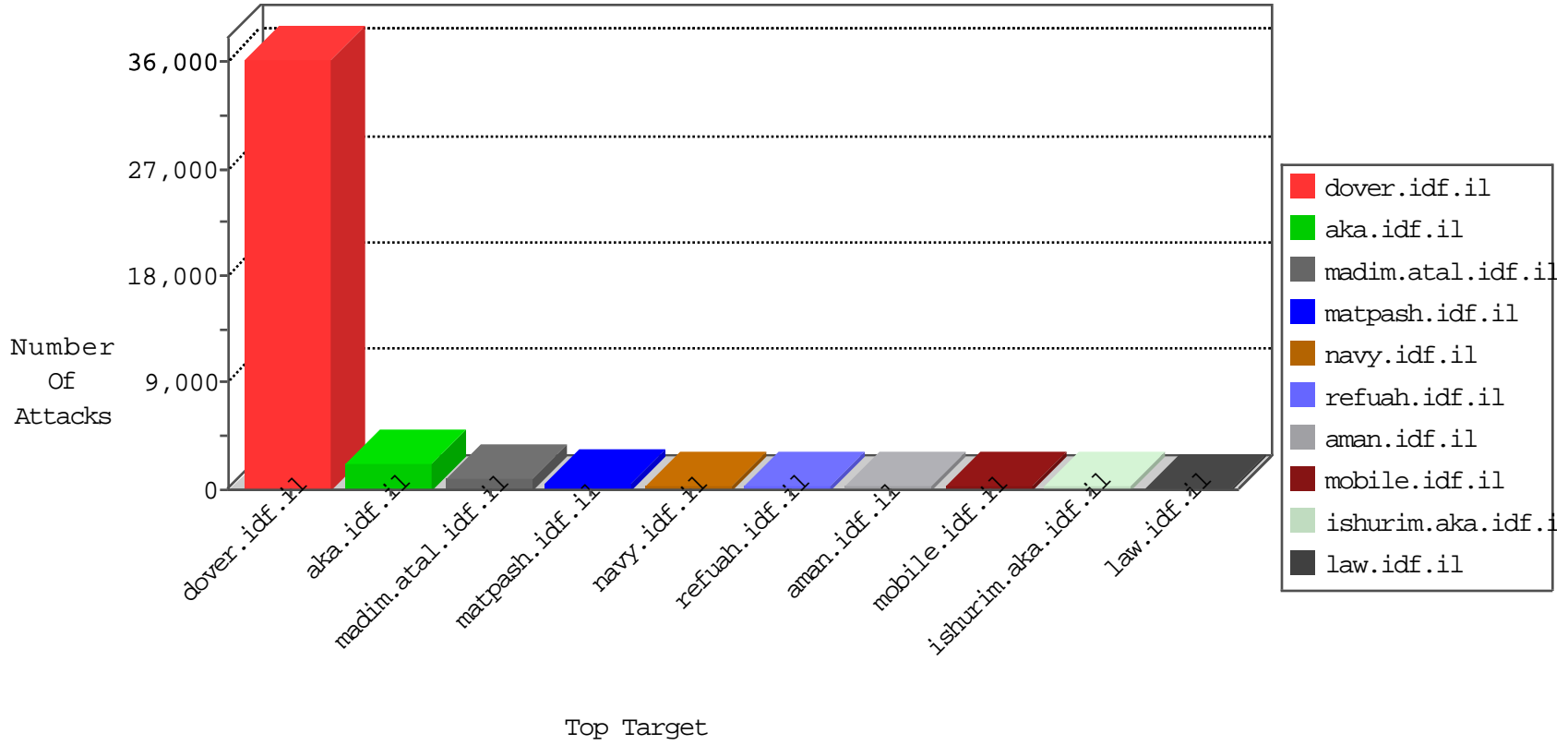


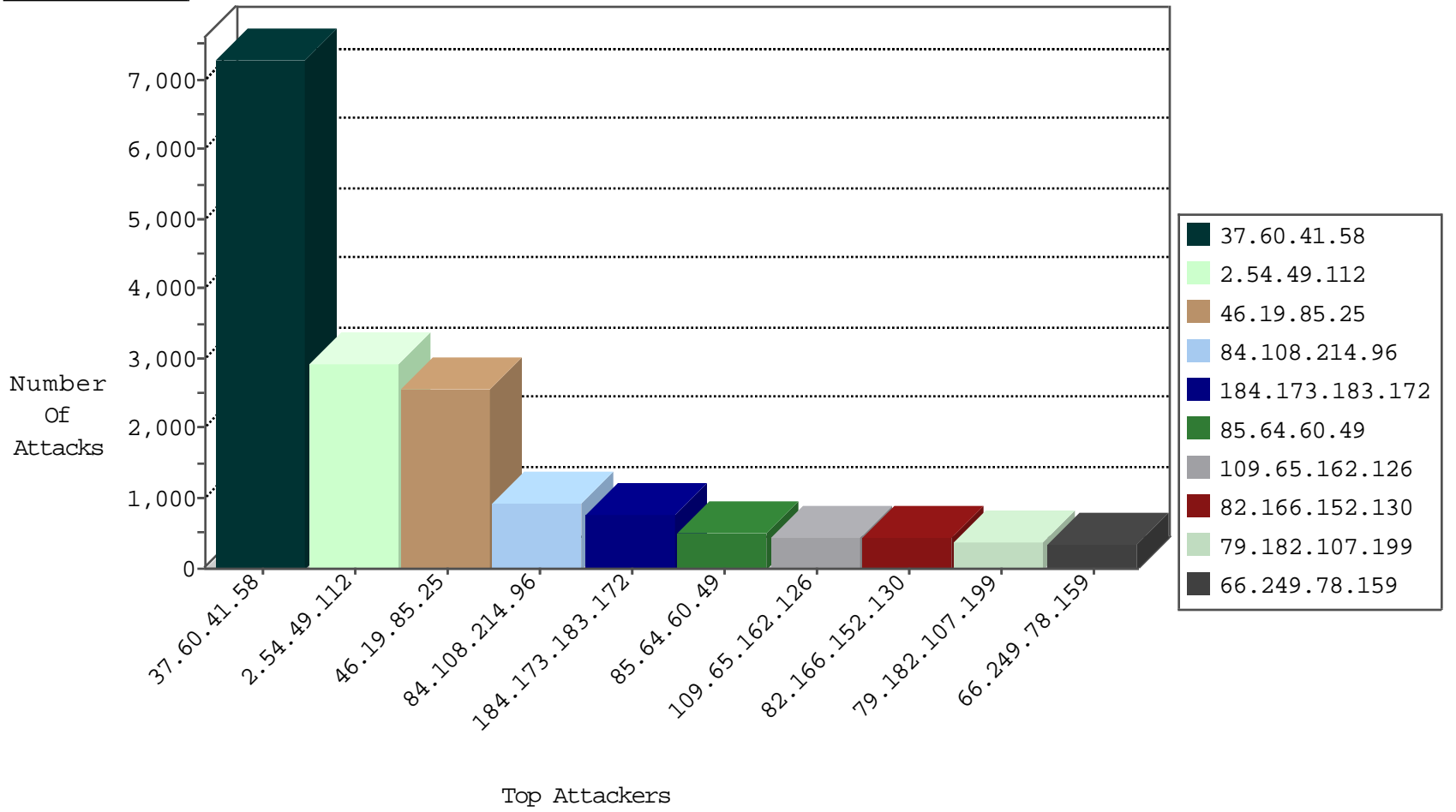
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.139	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6260
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5155
220.181.108.91	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3774
220.181.108.88	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3629
66.249.67.159	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3581
220.181.108.80	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3365
66.249.67.55	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3100
220.181.108.103	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3071
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1091
220.181.108.76	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1045
220.181.108.160	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	825
94.159.184.107	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	675
37.142.210.19	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	576
93.173.48.214	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	493
84.228.29.231	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	452
46.121.13.100	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	405
109.67.16.101	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	303
84.228.149.120	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
84.228.16.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	267
220.181.108.105	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	257
89.138.198.8	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	253
220.181.108.109	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	248
220.181.108.167	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	231
85.250.124.169	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	224
84.111.126.148	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
87.69.122.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	190
41.13.204.190	South Africa	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	189
220.181.108.91	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	183
220.181.108.176	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	177
109.186.181.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
212.235.79.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
87.68.53.235	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
220.181.108.143	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	163
79.180.175.184	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
85.250.228.53	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
91.150.104.251		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	161
80.178.13.60	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
85.250.167.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	128
109.67.71.12	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
220.181.108.184	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	127
220.181.108.108	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	123
87.68.86.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
220.181.108.179	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	118
220.181.108.100	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	118
109.65.195.89	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
220.181.108.147	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	110
149.78.125.90	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
46.19.86.128	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
87.68.54.186	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	491
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	292
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	232
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	152
84.94.41.129	Israel	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	70
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	18
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	11
46.116.163.178	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	6
46.117.248.136	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	6
85.250.79.201	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
46.120.114.48	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
91.220.131.130	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	4
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
195.142.179.50	Turkey	147.237.77.216	dover.idf.il	12373: HTTP: WordPress admin Login	Block	4
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
91.220.131.130	Russian Federation	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	4
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
58.59.238.250	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
91.220.131.130	Russian Federation	147.237.0.15	kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	4
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	4
80.246.138.203	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.176.170.49	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
91.220.131.130	Russian Federation	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	4
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
58.59.238.250	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
79.183.190.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
91.220.131.130	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	4

## Top Attackers In ID5

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	139
46.19.86.75	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	132
66.249.67.42	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
66.249.67.58	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
130.211.183.28		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.67.126	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.67.190	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
221.235.189.244	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	3
221.235.189.244	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	3
84.108.224.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.90.110.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.226.60.77	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
192.151.147.94	United States	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
77.126.117.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
66.249.73.201	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
81.218.126.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.121.64.34	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.244	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
46.117.78.138	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.245	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
192.151.147.94	United States	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
79.181.99.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.235.82	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.130.185.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
37.142.105.184	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.151.147.94	United States	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
149.78.101.26	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.151.147.94	United States	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
79.180.148.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.151.147.94	United States	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
2.54.188.200	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.67	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
79.178.137.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.151.147.94	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
217.132.213.111	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.216.28	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.90.215.60	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.144.133	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
66.249.78.60	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.244	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
213.57.109.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.34.169	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
37.60.41.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7296
2.54.49.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2792
46.19.85.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2556
84.108.214.96	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	933
85.64.60.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	519
82.166.152.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	443
105.188.57.211		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	262
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	245
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	240
87.163.160.92	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	217
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	211
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	199
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	197
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	192
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	168
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	162
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	157
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	151
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
188.195.145.220	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	141
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	139
84.250.128.236	Finland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	134
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	132
80.12.55.111	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	131
141.0.8.30	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	129
197.32.19.28	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	126
84.94.70.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	123
46.19.85.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
2.54.167.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
162.225.225.180	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	120
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	118
46.19.85.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	117
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	111
81.218.80.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
79.183.204.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	103
66.249.73.201	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	100
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
84.228.235.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	98
46.19.86.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	98
82.81.160.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
85.250.112.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
79.181.188.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	95
50.118.172.70	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	92
38.99.190.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	92
5.28.185.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	89
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	86
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	85
109.64.42.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.65.162.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	457
79.182.107.199	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.107.199	Block	391
176.12.136.91	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.136.91	Block	181
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	111
109.253.158.37	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.158.37	Block	73
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	62
109.253.149.26	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.149.26	Block	48
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	47
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	43
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	41
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	38
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	37
2.54.163.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	30
37.142.6.144	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.6.144	Block	25
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	25
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	24
77.125.208.50	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.208.50	Block	22
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	21
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	20
2.54.170.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	19
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
84.111.234.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	16
176.12.137.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	12
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
178.137.19.143	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	9
207.46.13.142	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.142	Block	9
162.243.108.228	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.108.228	Block	9
2.54.53.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	8
109.64.198.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7
157.55.39.64	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.64	Block	7
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	7
178.137.166.68	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	7
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	6
162.243.81.121	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.81.121	Block	6
84.110.110.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
94.153.9.66	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	6
157.55.39.81	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.81	Block	6
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	6
46.117.112.247	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/templates/getfile/	Block	5
37.142.143.82	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
203.133.170.144	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.170.144	Block	5
85.64.5.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	5
77.125.143.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	5
82.102.170.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	5
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	5
79.183.203.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4