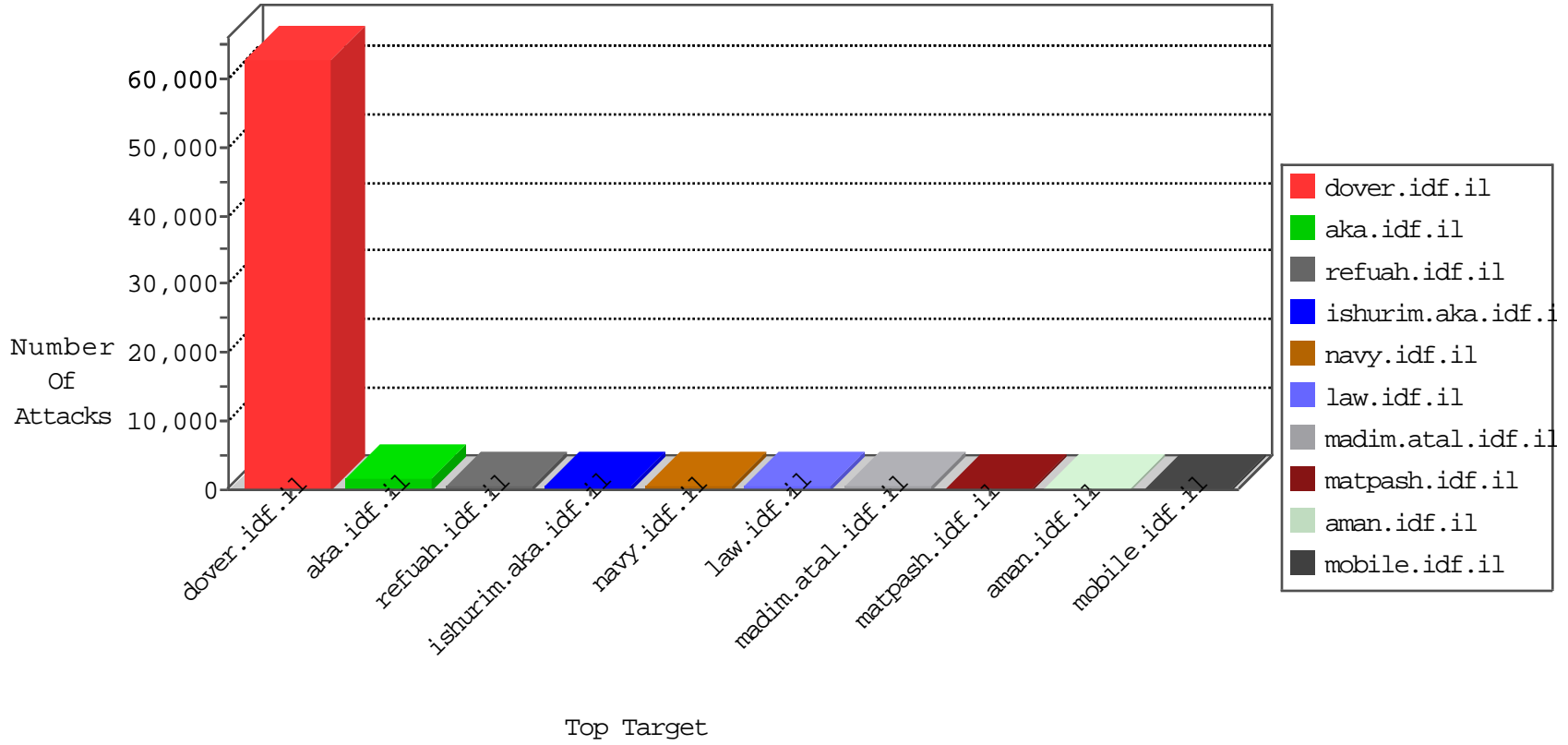


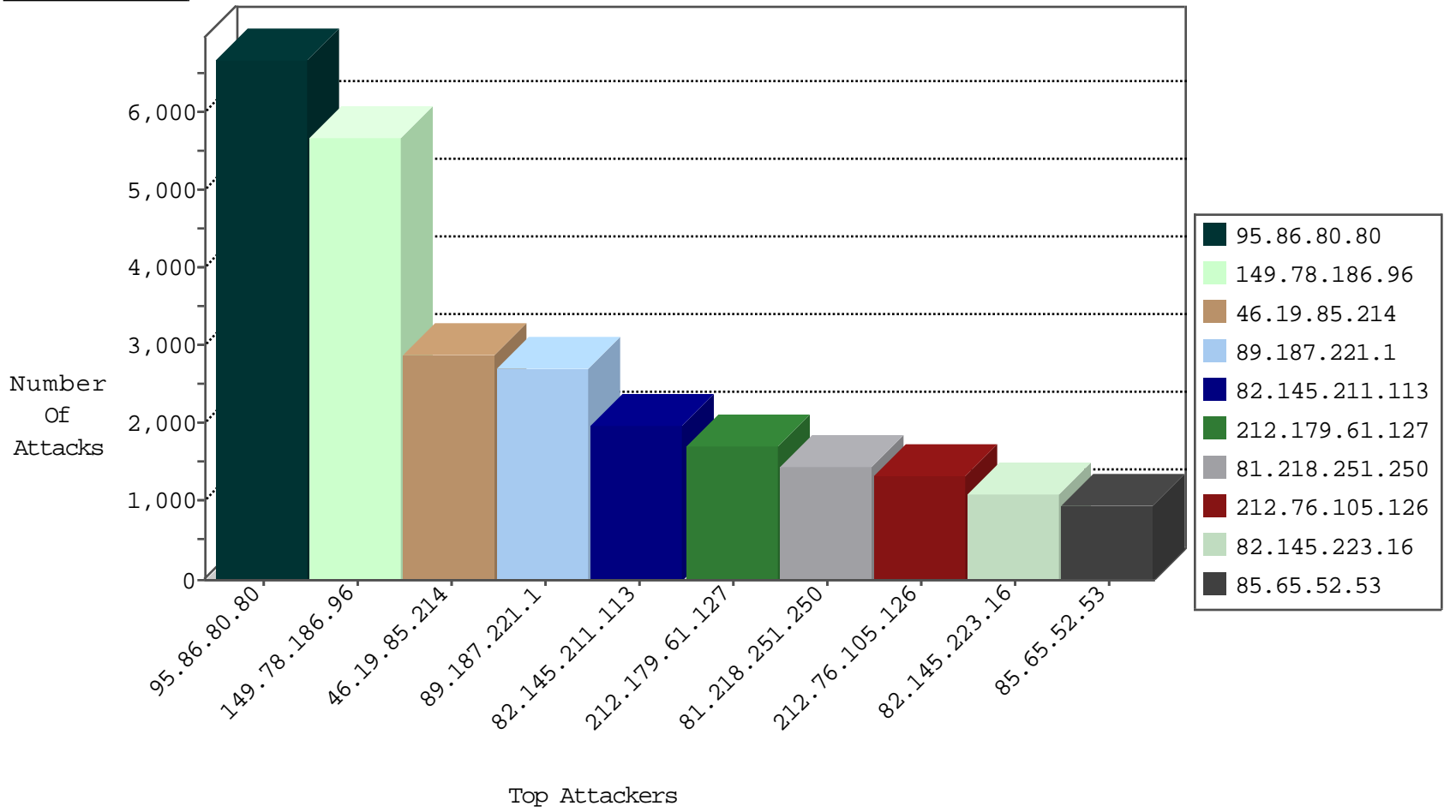
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15785
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	13572
157.55.39.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12509
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6648
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6537
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5108
173.252.73.116	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4746
66.249.67.159	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4209
220.181.108.159	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3482
66.249.67.190	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3021
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1907
220.181.108.105	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1376
220.181.108.107	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	882
220.181.108.86	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	716
220.181.108.152	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	633
77.125.109.17	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	586
220.181.108.160	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	464
220.181.108.165	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	401
46.121.120.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	353
66.249.67.139	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	257
87.68.22.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
84.109.165.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	229
149.88.102.174	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
213.57.248.78	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	195
213.57.250.140	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
93.172.101.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
220.181.108.169	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	180
220.181.108.157	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	178
84.109.39.30	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	176
220.181.108.123	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	168
46.120.5.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
84.111.168.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	143
178.197.232.45	Switzerland	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
213.57.150.194	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
84.228.83.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	134
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
213.57.150.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	123
5.29.171.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
109.67.207.44	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
95.86.83.21	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
220.181.108.101	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	97
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
46.19.86.210	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
37.142.128.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
87.69.227.181	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
176.12.143.117	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
85.64.224.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
220.181.108.116	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	79

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	294
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	138
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	135
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	134
77.125.87.150	Israel	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	126
184.173.183.172	United States	147.237.76.30	himush.idf.il	DVRep_P-N_40-59	Permit	121
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	78
204.44.65.104		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	27
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
59.175.238.8	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	15
106.185.44.134	Japan	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	9
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	9
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	8
212.34.12.124	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
79.177.41.10	Israel	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	7
106.185.44.134	Japan	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
213.57.103.30	Israel	147.237.72.166	aka.idf.il	1106: HTTP: IIS ..%c Encoded \ in URI	Permit	6
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.198	e.yochalan.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
94.230.86.243	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.64.45.216	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.228.130.106	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
197.162.14.7	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
115.188.138.186	New Zealand	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.117.63.215	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
79.182.152.14	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.189	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
89.139.190.1	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.76.38	e.e.meitav.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	139
46.117.221.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	10
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
213.57.15.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
109.186.27.105	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
66.249.67.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.65.9	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
188.138.9.51	Germany	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	3
66.249.67.126	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
88.198.5.141	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
144.0.0.60	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.55	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.243	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
46.116.174.45	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.4	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.242	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
144.0.0.60	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
176.12.150.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.172.249	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
218.77.79.43	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
37.26.147.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
84.94.60.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.104.110.103	Iran, Islamic Republic of	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 2048	2
79.179.106.146	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.158.181	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
80.246.133.241	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
178.19.107.114	Poland	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.172	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
144.0.0.60	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
95.86.67.226	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.172.60	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
196.26.82.212	South Africa	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
221.235.189.245	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.31	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
88.198.5.141	Germany	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
87.68.77.142	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
95.86.80.80	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6675
149.78.186.96	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5677
46.19.85.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2890
89.187.221.1	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2706
82.145.211.113	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1968
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1721
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1449
212.76.105.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1348
82.145.223.16	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1101
85.65.52.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	958
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	827
149.78.88.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	675
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	585
193.106.54.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	555
164.138.121.87	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	540
2.52.144.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	537
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	517
41.54.80.172	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	491
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	412
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	384
79.181.173.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	332
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	331
31.168.71.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	306
157.150.193.2	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	285
41.79.120.16	N/A	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	278
46.19.85.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	269
46.19.86.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	260
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	231
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	225
80.230.69.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	224
139.11.10.122	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	224
37.231.181.190	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	216
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	209
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	202
79.177.26.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	199
2.36.92.236	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	198
213.57.252.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	180
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167
82.145.221.223	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	164
46.19.86.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	163
104.131.228.99		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	163
180.254.223.252	Indonesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	156
195.241.159.215	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	149
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	144
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	142
162.243.222.48	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	141
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
70.196.5.67	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	129
2.54.50.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	128
109.67.207.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	126

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.101	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.101	Block	266
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	101
176.12.145.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.145.210	Block	82
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	81
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	66
109.253.134.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	31
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	23
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	17
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	14
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	13
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
81.144.138.34	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.144.138.34	Block	11
95.86.98.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	11
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
95.86.116.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
192.116.199.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	8
157.55.39.152	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/captcha.ashx	Block	8
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
79.176.152.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	6
106.185.44.134	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 106.185.44.134	Block	6
95.86.66.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
95.86.116.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/<html><head><title>502 bad gateway</title></head><body bgcolor=	Block	6
109.67.66.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	6
157.55.39.255	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 157.55.39.255	Block	6
93.172.27.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	5
114.215.133.202	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	5
79.180.127.108	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.180.127.108	Block	5
157.55.39.6	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	5
207.46.13.26	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.26	Block	5
106.185.44.134	Japan	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 106.185.44.134	Block	5
95.86.116.51	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.116.51	Block	5
79.181.183.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
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	5
109.67.207.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/print_text.asp	Block	5
157.55.39.182	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.182	Block	5
106.185.44.134	Japan	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 106.185.44.134	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	4
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
82.166.20.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
207.46.13.99	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	4
94.230.92.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
31.44.136.66	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
109.160.219.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
74.50.21.240	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.50.21.240	Block	4
79.180.127.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	4