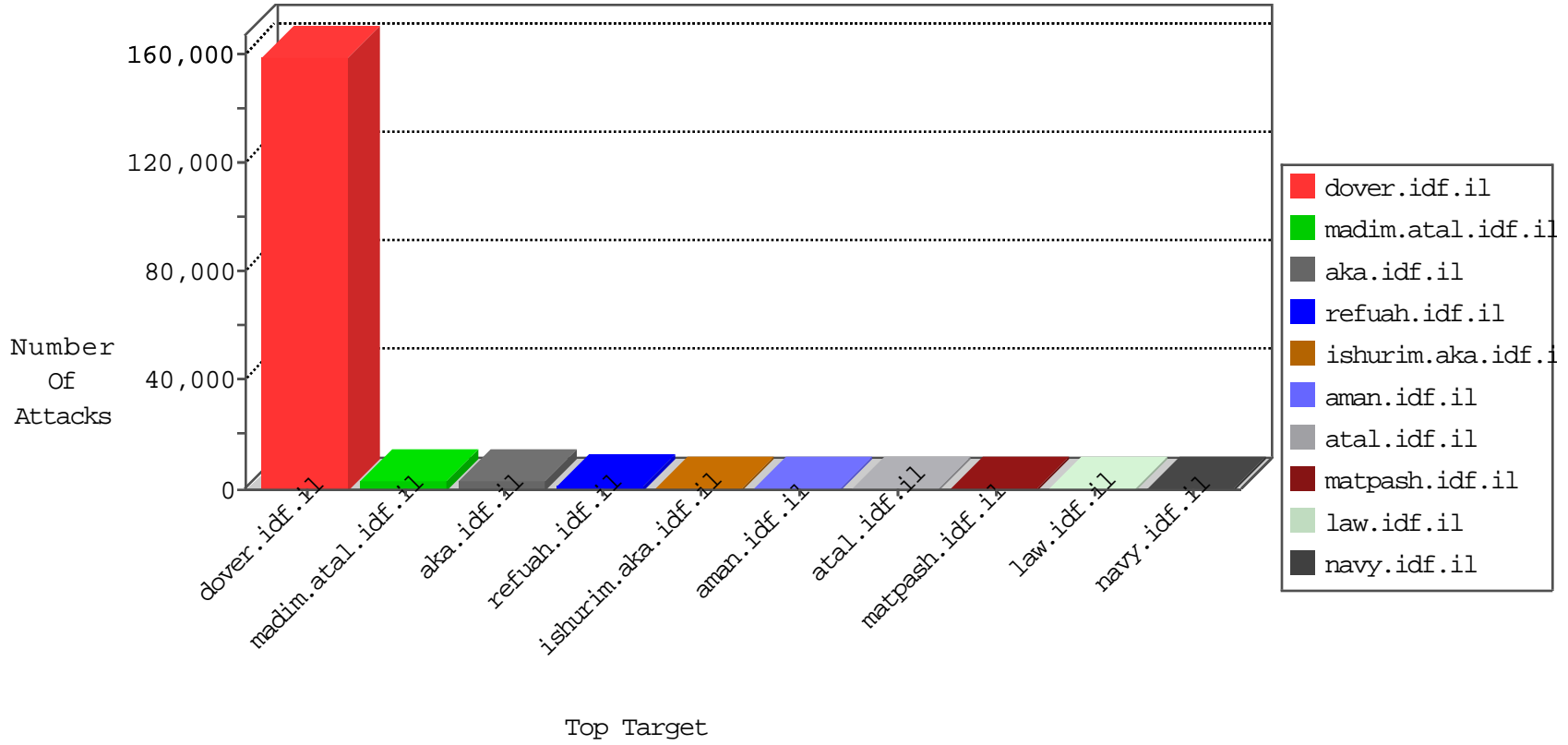


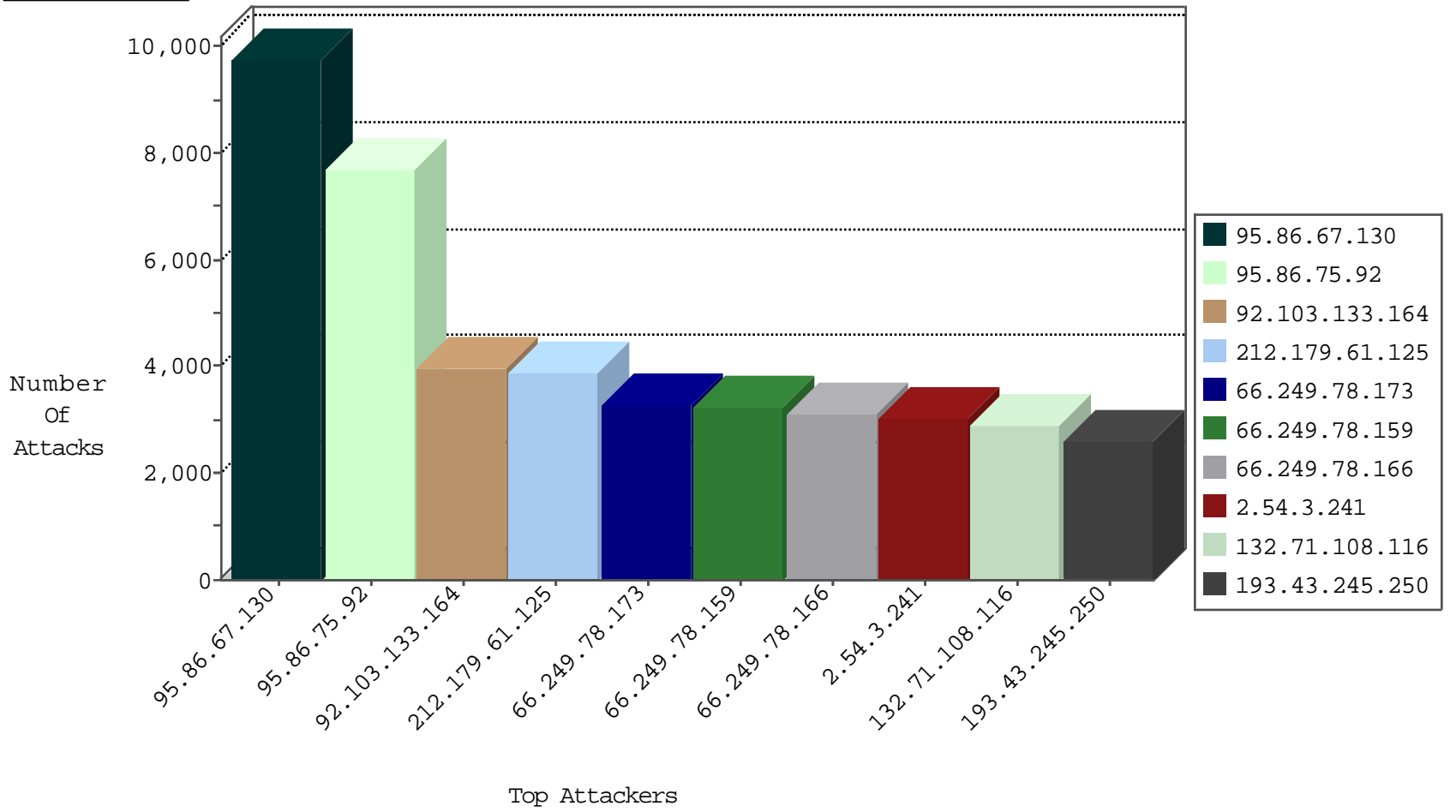
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
220.181.108.109	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	18683
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	8313
66.249.79.34	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8303
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	4908
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3761
66.249.79.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3328
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3130
66.249.79.42	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2746
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2367
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1864
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1532
66.249.79.13	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1148
79.177.31.71	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	866
79.181.48.85	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	736
66.249.67.39	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	732
213.57.238.250	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	732
220.181.108.144	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	438
77.127.2.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	418
220.181.108.145	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	403
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	392
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	385
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	382
149.88.86.62	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	374
109.65.5.81	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	319
37.142.143.95	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	314
79.182.182.171	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	313
66.249.64.142	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	273
109.66.61.248	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	271
212.25.123.18	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	263
84.229.30.43	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	255
89.139.52.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
213.57.104.56	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	233
79.178.107.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
213.57.232.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
79.183.116.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
109.64.110.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	162
5.22.135.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	141
109.160.180.177	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	137
220.181.108.171	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	119
79.180.194.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
82.102.141.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	110
213.57.39.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
46.117.195.224	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	109
46.116.211.237	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	108
85.65.52.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
46.116.170.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	106
46.121.58.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	547
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	55
79.177.122.133	Israel	147.237.76.42	refuah.idf.il	C1000208: HTTP: Range in the Header	Block	24
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	19
62.90.220.150	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	13
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
82.166.226.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
37.59.19.32	France	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	9
49.151.53.125	Philippines	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
180.76.5.193	China	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	8
2.54.28.35	Israel	147.237.77.216	dover.idf.il	C1000208: HTTP: Range in the Header	Block	7
84.108.184.149	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
31.25.143.180	Iraq	147.237.77.216	dover.idf.il	C1000208: HTTP: Range in the Header	Block	6
77.125.252.254	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
180.190.131.94	Philippines	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.179.61.124	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
5.29.161.150	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.197	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	6
85.250.7.185	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
82.80.128.20	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.34.12.151	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
82.80.135.182	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
212.34.12.191	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	5
80.178.2.74	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.224	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
109.160.225.135	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
109.253.135.8	Israel	147.237.76.31	nakchal.idf.il	C1000208: HTTP: Range in the Header	Block	4

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	193
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	105
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	98
66.249.79.89	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	97
66.249.79.132	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	70
46.19.86.145	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	26
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	23
217.21.15.11	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	19
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	12
209.236.121.57	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	9
66.249.79.5	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	8
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	6
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
91.227.71.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.79.157	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.74	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	3
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
58.20.54.249	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.130	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.81	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.163	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.163	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.79.13	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
164.138.120.74	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.31	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
81.218.55.253	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.64.76	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
84.111.234.58	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.123.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.148	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
60.208.72.139	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
43.255.191.163	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
79.178.51.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.188.210	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.73	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
5.28.145.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.76	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
46.121.142.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
2.54.163.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.39	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.163	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.212	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
89.139.23.28	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
95.86.67.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9767
95.86.75.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7695
92.103.133.164	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3974
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3860
2.54.3.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2994
132.71.108.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2896
193.43.245.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2611
193.43.246.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2464
213.57.240.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2403
82.145.221.61	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2198
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2029
109.65.48.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1971
84.95.199.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1948
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1916
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1913
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1890
212.179.42.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1779
80.184.4.182	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1767
80.94.146.48	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1725
95.86.118.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1646
81.218.131.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1582
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1480
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1131
82.145.220.148	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1107
79.181.30.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1106
79.176.165.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1014
31.25.143.180	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	987
82.145.223.76	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	977
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	925
46.19.85.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	866
212.179.180.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	819
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	784
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	746
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	730
2.54.140.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	729
2.54.163.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	729
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	693
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	690
164.138.119.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	659
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	649
212.179.21.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	561
80.184.79.107	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	555
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	546
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	528
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	527
212.179.61.124	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	497
77.127.201.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	495
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	483
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	475
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	463

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.117.26.204	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.26.204	Block	750
84.108.8.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	585
2.54.173.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	497
37.26.147.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	335
213.57.55.88	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.55.88	Block	261
2.54.129.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
109.253.157.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	105
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.34	Block	103
176.12.143.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	86
31.168.214.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/&	Block	81
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	75
176.12.140.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
109.253.134.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
109.253.139.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
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	34
109.253.132.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
80.246.139.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
85.250.52.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	23
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	22
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	20
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	19
62.90.140.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	18
176.12.147.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
95.86.112.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	18
77.127.95.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
176.12.150.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
149.78.85.141	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.85.141	Block	16
62.219.141.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	14
209.236.121.57	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	14
207.46.13.78	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
212.179.214.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
66.249.79.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
2.54.36.241	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.36.241	Block	10
207.46.13.133	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
212.179.61.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
109.253.133.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
207.46.13.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.77	Block	9
79.177.60.197	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	9
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	8
85.65.177.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	7
207.46.13.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.133	Block	7
93.173.28.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
157.55.39.206	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
109.66.110.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	7
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	7
109.253.143.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7