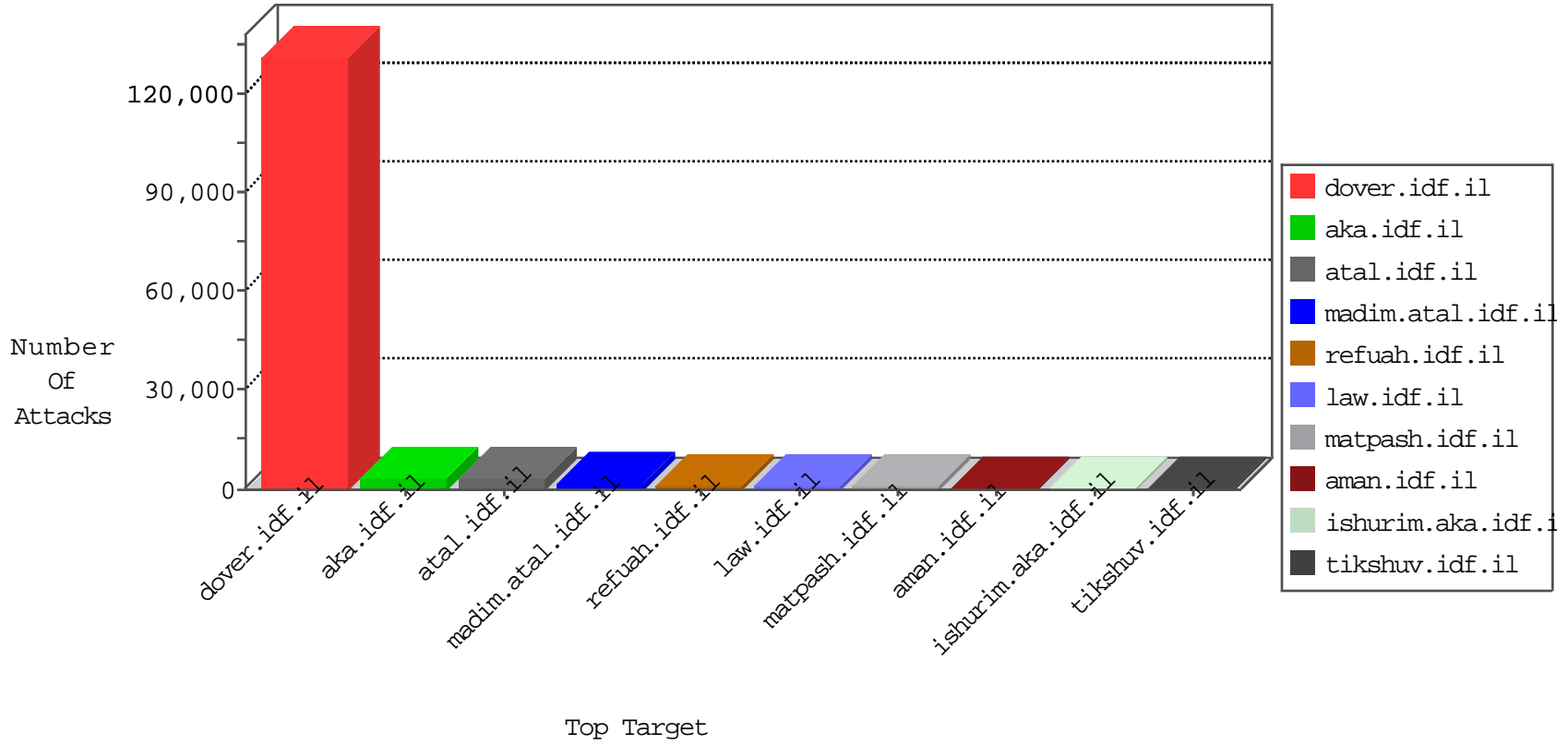


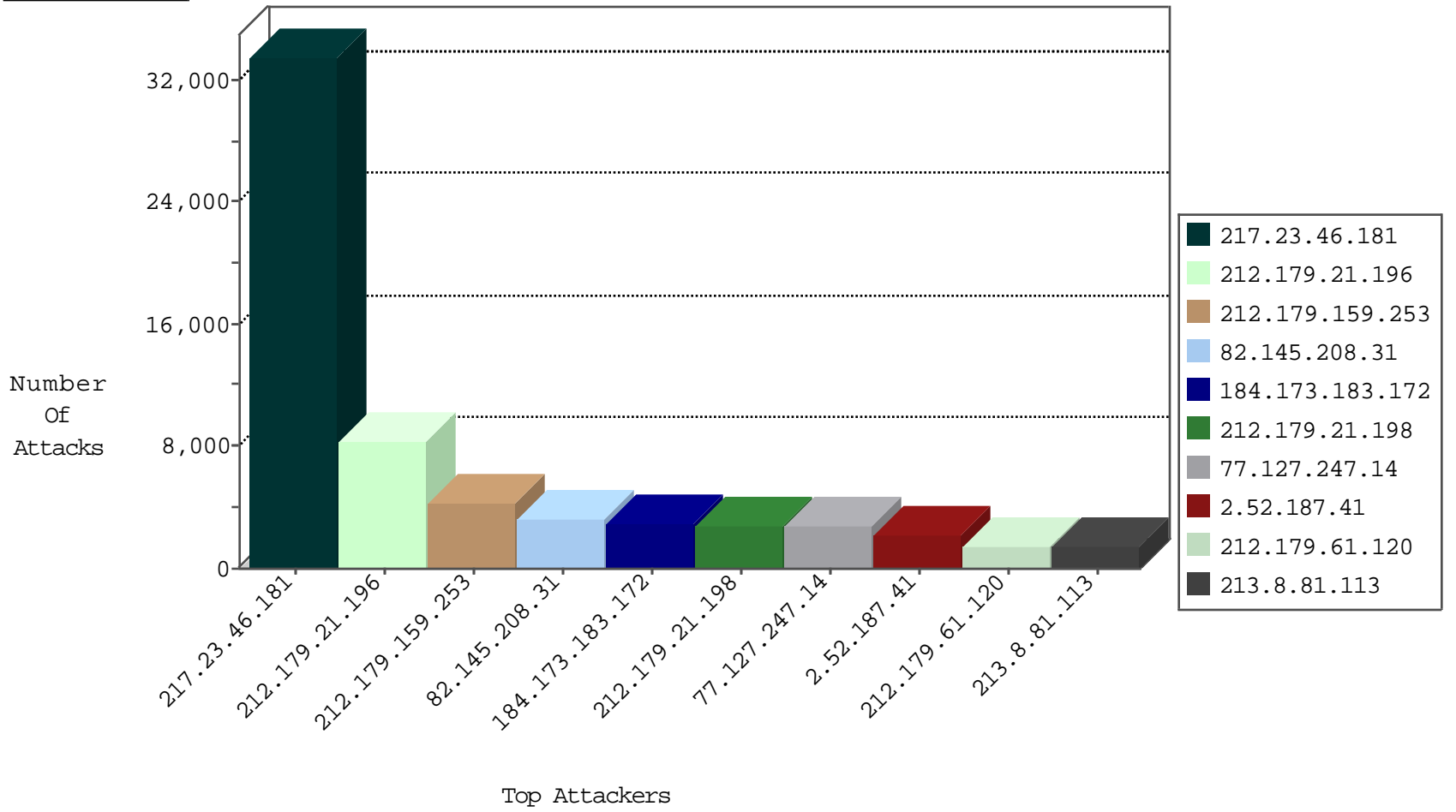
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
220.181.108.97	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	4317
220.181.108.140	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	4052
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2954
66.249.64.156	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2931
46.19.86.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2747
82.166.184.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2666
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2660
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	955
46.120.128.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	618
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	558
132.64.210.76	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	480
79.180.193.228	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	453
109.186.181.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	362
213.57.109.65	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	336
212.199.156.81	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	332
79.179.2.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	264
77.127.151.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	254
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	252
79.179.124.94	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	242
220.181.108.90	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	223
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	222
80.178.154.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	206
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
212.76.101.201	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	194
220.181.108.93	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	193
192.114.2.35	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
220.181.108.118	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	177
185.32.176.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	174
220.181.108.172	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	174
46.120.80.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
109.186.182.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
147.235.185.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
84.108.204.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	132
105.157.5.71	Morocco	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	119
85.64.15.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
2.54.151.19	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
87.68.40.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
37.26.147.217	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
85.250.228.53	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
37.142.129.150	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	81
79.183.195.44	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
109.64.27.54	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
109.64.109.68	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
2.52.22.106	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
2.54.189.147	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
79.176.55.127	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
80.246.138.89	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
220.181.108.179	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	69
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	66
194.90.239.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	65

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.145.208.31	Europe	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2950
77.127.247.14	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2506
2.52.187.41	Israel	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	2078
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	717
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	676
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	540
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	512
77.127.247.14	Israel	147.237.72.166	aka.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	235
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	166
180.76.5.193	China	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	162
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	120
2.52.187.41	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	117
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	49
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
212.199.97.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	27
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	23
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	anan.idf.il	DVRep_P-N_40-59	Permit	20
46.117.102.106	Israel	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	8
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	7
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	6
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	6
77.125.158.12	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	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	6
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	6
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
79.183.148.132	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.59.150.121	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
46.121.197.129	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	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
46.19.86.161	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.76.176	test.noore.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
81.218.251.252	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
41.185.12.165	South Africa	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.205	prisha.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	98
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	55
144.76.206.245	Germany	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
156.17.187.240	Poland	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	35
2.52.131.238	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
178.238.235.184	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	11
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
66.249.64.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
46.19.85.102	Israel	147.237.76.42	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
46.117.62.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	3
46.4.105.45	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
79.179.153.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	3
176.106.44.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	3
178.77.125.84	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.69.58	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.83	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
82.166.100.209	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
176.31.126.12	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
118.163.104.56	Taiwan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
46.116.214.179	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
200.62.212.243	Peru	147.237.72.166	aka.idf.il	SERVER-WEBAPP backup access	2
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
176.12.139.255	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
2.54.190.53	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
66.249.64.63	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
144.0.0.60	China	147.237.76.201	e.atal.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
79.179.5.137	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
84.108.174.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
91.224.132.118	Russian Federation	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
77.125.122.211	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	2
46.117.125.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
221.235.189.244	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.46	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
200.62.212.243	Peru	147.237.76.31	nakchal.idf.il	SERVER-WEBAPP backup access	2
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
149.78.109.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
66.249.64.161	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
79.182.27.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32897
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8206
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4258
212.179.21.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2825
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1475
213.8.81.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1456
212.179.42.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1043
66.87.115.65	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	935
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	818
109.64.160.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	799
2.54.176.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	793
109.110.118.146	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	782
31.44.129.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	743
132.70.40.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	729
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	713
81.218.116.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	687
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	631
82.166.102.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	623
94.159.206.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	615
109.65.116.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	603
155.140.133.214	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	566
82.145.221.145	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	561
217.65.199.81		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	524
92.103.133.164	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	509
192.116.83.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	500
77.125.158.12	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	499
82.80.222.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	487
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	466
203.104.11.21	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	448
78.108.169.23	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	417
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	408
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	397
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	396
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	364
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	342
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	334
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	331
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	327
2.52.35.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	323
157.150.192.237	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	310
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	299
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	292
134.159.156.68	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	276
79.173.193.134	Jordan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	270
192.115.177.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
82.145.208.141	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	260
194.177.16.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	253
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	244

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.188.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	662
37.26.147.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	333
2.54.189.131	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.189.131	Block	282
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	200
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	192
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	187
185.32.177.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	129
176.12.139.89	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.139.89	Block	118
176.12.140.69	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.140.69	Block	105
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 217.23.46.181	Block	98
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	88
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	81
80.246.138.52	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.138.52	Block	74
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.128	Block	63
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	49
144.76.206.245	Germany	147.237.72.166	aka.idf.il	PHP Attempt	Block	48
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	43
79.177.162.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	37
79.180.210.212	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	36
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	27
2.54.163.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	25
144.76.206.245	Germany	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 144.76.206.245	Block	23
213.151.48.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	23
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	21
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	17
149.78.26.190	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	17
213.151.53.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	17
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
84.110.209.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.110.209.225	Block	16
62.0.1.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
200.62.212.243	Peru	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	14
84.228.152.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	13
200.62.212.243	Peru	147.237.72.166	aka.idf.il	PHP Attempt	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/print_text.asp	Block	12
37.60.42.222	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
82.80.222.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	12
109.186.5.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	11
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	11
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	11
213.57.50.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	11
209.36.43.66	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
80.178.11.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
79.182.155.191	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.182.155.191	Block	9
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	8
46.117.4.178	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	8