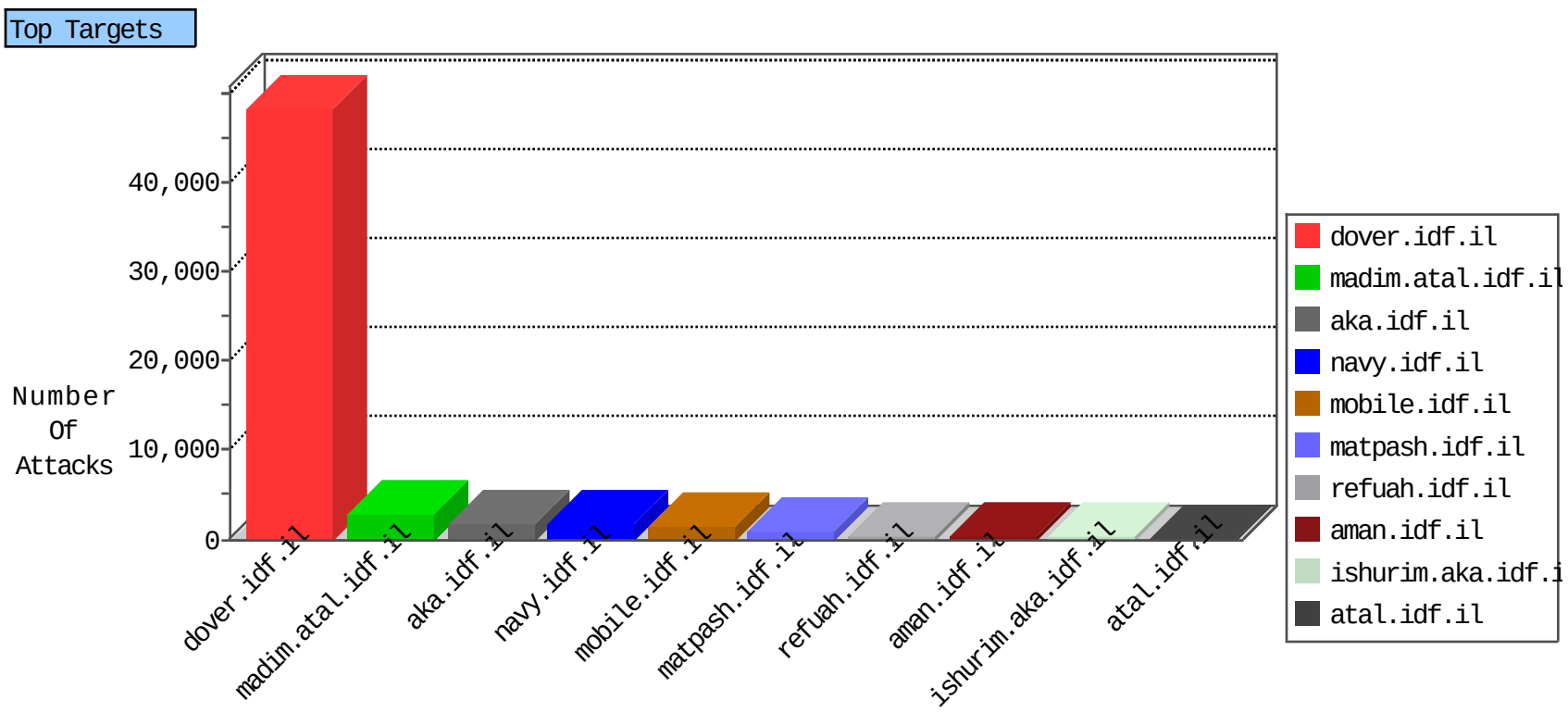
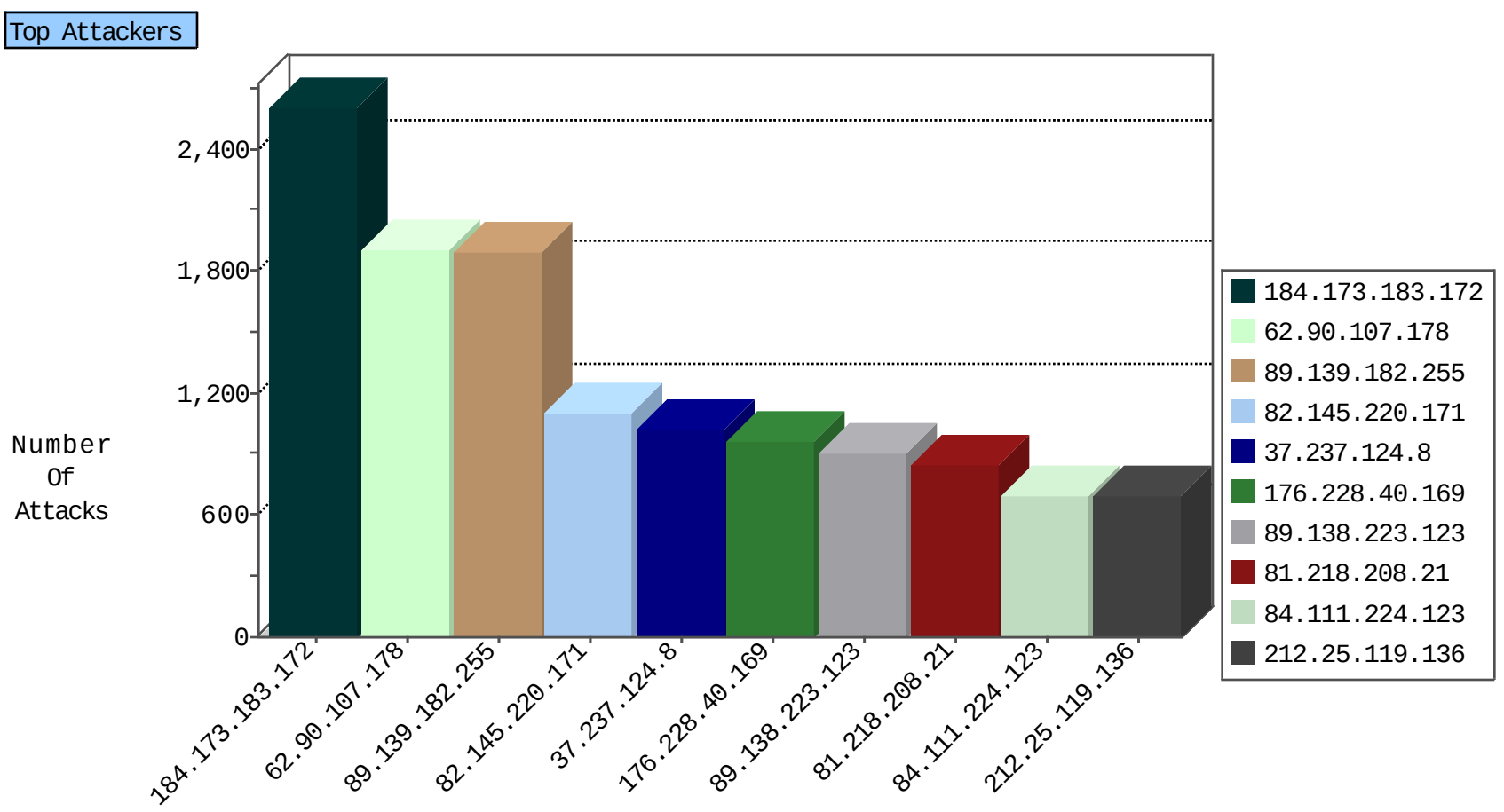
05-30-2015-00:00:08 to 05-31-2015-00:00:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-30-2015-00:00:08 to 05-31-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
41.44.105.185	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4286
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3490
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3260
66.249.78.60	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2647
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	903
67.142.163.22	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	589
216.218.206.66	United States	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	584
93.172.9.85	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	446
79.177.127.111	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	305
79.179.103.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
220.181.108.165	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	228
37.142.11.140	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	212
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	209
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
220.181.108.155	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	201
2.52.133.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
46.188.121.29	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	190
217.194.197.200	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	184
79.180.97.211	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
5.29.176.182	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	172
2.52.151.103	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
220.181.108.163	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	165
46.120.76.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	157
213.57.109.33	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	155
46.19.86.235	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	155
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	147
79.183.16.15	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	139
176.12.138.74	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	139
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
220.181.108.82	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	130
81.207.195.213	Netherlands	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	130
132.66.222.132	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
212.179.61.126	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	115
46.120.245.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
84.111.48.97	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	110
109.186.75.146	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
213.57.137.121	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
2.54.26.187	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
109.65.52.11	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
220.181.108.148	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	101
80.74.107.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
5.144.59.192	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
79.183.116.199	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
84.109.152.163	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.19.86.239	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
2.52.132.136	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
2.52.191.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
79.183.169.36	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80

05-30-2015-00:00:08 to 05-31-2015-00:00:08

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	1471
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	873
64.79.144.10	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	386
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	266
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	197
89.139.182.255	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	51
87.69.52.151	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	32
125.79.138.126	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	25
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
175.44.6.111	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	19
46.118.157.21	Ukraine	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	15
212.34.12.184	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	11
218.106.246.229	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Permit	8
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	7
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	6
37.46.39.69	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
77.126.15.131	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	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	5
109.186.60.116	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	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
5.29.60.20	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.200.171.116	Jordan	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	5
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
109.186.53.172	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.135.131	United States	147.237.8.14	e.orchot.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
66.240.192.138	United States	147.237.8.14	e.orchot.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
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
79.176.103.114	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
195.210.47.173	Kazakstan	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	4
58.59.235.176	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4

05-30-2015-00:00:08 to 05-31-2015-00:00:08

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	269
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.79.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
176.31.245.16	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.69.63	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
149.78.134.249	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
202.148.12.117	Indonesia	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
37.237.124.8	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	4
66.249.79.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
218.106.246.229	China	147.237.77.216	dover.idf.il	SERVER-WEBAPP mod-plsql administration access	4
103.12.96.13	Afghanistan	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.144	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
202.148.12.117	Indonesia	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
85.108.4.179	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
186.101.25.218	Ecuador	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
43.255.188.130	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
186.101.25.218	Ecuador	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	3
186.101.25.218	Ecuador	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
94.159.234.213	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.204.117	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
202.148.12.117	Indonesia	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
187.216.192.195	Mexico	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
80.230.110.74	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
87.68.24.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.130	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
115.28.143.12	China	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.117.71.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.14	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
202.148.12.117	Indonesia	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.116.101.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.130	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
2.54.30.181	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
140.126.196.179	Taiwan	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.19.86.136	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.79.172	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
202.148.12.117	Indonesia	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
61.183.128.6	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
115.28.143.12	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.188.130	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
150.67.4.236	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
202.148.12.117	Indonesia	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

05-30-2015-00:00:08 to 05-31-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
62.90.107.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1906
89.139.182.255	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1839
82.145.220.171	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1106
37.237.124.8	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1009
176.228.40.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	968
89.138.223.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	900
81.218.208.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	840
212.25.119.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	692
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	635
2.52.161.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	559
31.168.64.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	549
82.145.218.226	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	505
95.86.122.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	469
93.173.243.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	441
70.39.187.8	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	428
94.159.157.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	405
2.54.37.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	390
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	388
82.145.217.239	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	386
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	383
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	378
46.19.86.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	368
37.239.68.81	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	356
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	334
82.145.223.113	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	294
46.19.85.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	251
46.19.85.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	243
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	239
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	225
109.65.135.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	210
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	210
84.228.34.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	186
148.177.129.210	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	182
95.133.130.82	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167
93.173.28.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	165
67.142.163.22	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	162
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159
2.54.183.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159
109.110.113.22	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	153
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	149
172.56.17.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	144
46.19.86.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	141
46.19.86.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
79.179.0.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	128
93.172.58.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	126
50.118.162.165	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
2.54.145.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	115
149.78.112.246	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	113
197.205.70.145	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	112
46.116.193.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	111

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.111.224.123	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.111.224.123	Block	698
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	383
77.126.15.164	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.126.15.164	Block	308
213.57.137.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	243
79.181.25.29	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.181.25.29	Block	233
37.142.85.73	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.142.85.73	Block	222
79.182.113.67	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.182.113.67	Block	211
2.54.27.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	187
2.54.4.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	152
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	110
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	88
85.65.225.211	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.65.225.211	Block	84
79.182.113.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	82
84.94.83.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	74
80.246.138.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.86.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	70
79.183.48.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	63
109.253.128.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	47
2.54.167.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	47
46.19.85.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	42
2.54.148.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	42
2.54.144.28	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	40
79.180.123.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	37
84.109.11.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	32
46.121.17.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	31
176.12.146.124	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	29
84.228.67.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	29
93.173.249.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	29
77.126.15.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
85.250.18.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	27
93.172.191.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	27
2.54.189.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	25
2.52.157.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	22
46.19.86.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	22
79.181.10.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	19
109.67.31.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	19
46.120.54.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	17
93.173.227.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	17
93.173.146.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	17
84.111.81.96	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.111.81.96	Block	16
37.142.150.43	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	16
85.64.152.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.152.139	Block	16
93.172.22.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
79.177.3.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
185.32.176.119	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
176.12.151.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
176.12.146.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
218.106.246.229	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 218.106.246.229	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
2.54.44.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14