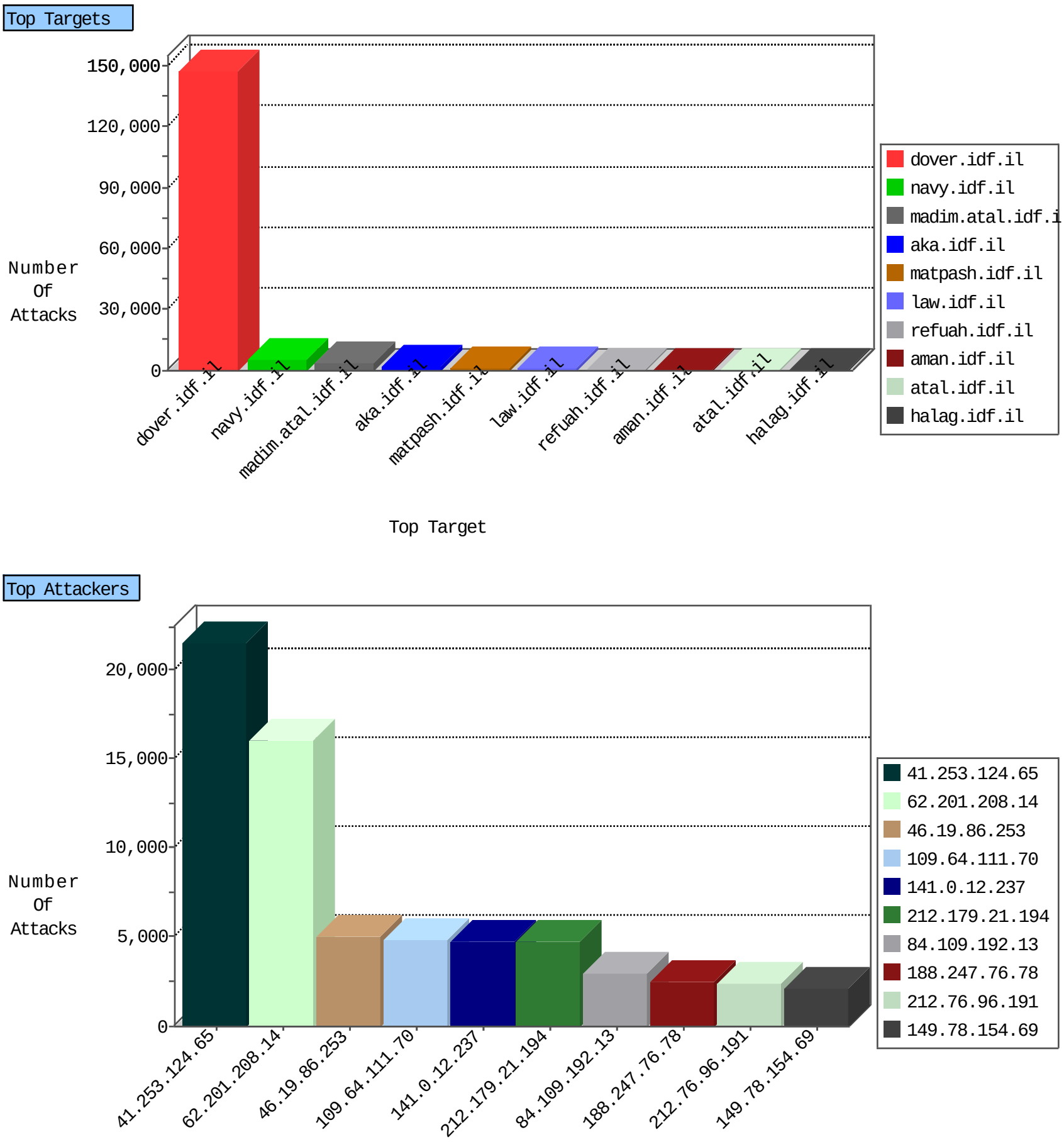
06-18-2015-00:00:07 to 06-19-2015-00:00:07

IDF Under Attack Daily Report



06-18-2015-00:00:07 to 06-19-2015-00:00:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
79.182.129.44	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3267
46.116.147.54	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3225
188.247.76.78	Jordan	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3184
80.230.79.175	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2670
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2563
220.181.108.102	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	778
46.120.31.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	663
66.187.72.219	United States	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	629
66.249.65.65	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	598
141.0.12.237	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	496
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	485
66.249.65.176	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	430
220.181.108.123	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	419
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	315
79.178.208.61	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	284
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	260
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	256
79.178.149.68	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	239
41.238.32.104	Egypt	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	201
41.253.124.65	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	181
199.203.172.65	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
5.22.130.199	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	165
93.173.139.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
85.65.32.11	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
213.8.71.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	143
79.181.193.8	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
77.127.206.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
62.0.25.121	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	128
87.68.54.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
147.235.236.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
85.250.57.222	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	122
185.32.178.152	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
192.114.91.245	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	116
85.130.230.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
79.181.57.8	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
109.186.80.179	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	113
37.142.5.70	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	107
5.29.171.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
46.19.86.253	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
37.187.157.108	France	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	98
37.142.134.75	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
46.19.85.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	95
185.32.178.18	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
46.19.85.92	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
109.253.129.88	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
80.246.136.112	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
176.12.141.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
2.54.128.214	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
46.19.86.90	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
192.115.141.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85

06-18-2015-00:00:07 to 06-19-2015-00:00:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.111.70	Israel	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	4511
77.125.87.150	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	550
109.64.111.70	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	354
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	243
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	232
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	189
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	185
184.173.183.172	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	139
37.59.19.32	France	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	119
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	108
118.123.11.45	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
31.13.163.43	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	25
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	23
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
2.52.20.250	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	16
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
46.117.159.41	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
2.52.20.250	Israel	147.237.0.15	kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	8
83.111.35.201	United Arab Emirates	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
37.142.197.138	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.116.188.226	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	6
79.182.129.44	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.132.47.162	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	5
93.173.236.177	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
181.171.205.135	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.29.51.176	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
2.52.20.250	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	5
85.250.208.19	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	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
46.116.183.134	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	4
85.130.245.124	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	4

06-18-2015-00:00:07 to 06-19-2015-00:00:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
188.247.76.78	Jordan	147.237.77.216	dover.idf.il	SERVER-WEBAPP Cisco /%% DOS attempt	2324
66.249.90.46	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	654
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	103
66.249.84.146	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	8
85.250.140.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	7
188.247.76.78	Jordan	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	6
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
154.121.251.242		147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	3
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.188.135	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
193.28.199.59	Germany	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
212.106.64.62	Palestinian Territory, Occupied	147.237.77.176	matpash.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
43.255.188.131	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
109.253.149.155	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
61.240.144.66	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.144	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
218.24.171.223	China	147.237.76.197	e.himush.idf.il	GPL SCAN nmap TCP	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.65	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.146	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
79.183.19.50	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.132	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
79.182.129.44	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.67	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.135	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.179	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.132	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.161	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
192.3.108.133	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
109.253.149.155	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	2
66.249.73.225	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.65.68	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
188.247.76.78	Jordan	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.132	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
132.66.40.116	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.131	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2

06-18-2015-00:00:07 to 06-19-2015-00:00:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.253.124.65	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21274
62.201.208.14	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16010
46.19.86.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5046
141.0.12.237	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4787
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4706
84.109.192.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2991
212.76.96.191	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2437
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2128
70.39.186.107	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1684
85.250.140.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1618
132.64.4.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1129
95.86.100.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1093
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1081
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1081
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1029
2.52.19.100	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1009
82.145.222.83	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	892
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	833
79.182.129.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	823
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	716
79.181.169.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	649
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	621
132.71.142.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	619
2.52.156.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	607
212.179.61.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	588
66.249.84.182	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	563
66.249.84.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	549
46.19.86.160	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	546
37.26.147.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	543
85.250.223.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	543
66.249.84.188	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	541
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	497
194.138.39.62	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	467
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	461
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	446
149.255.192.46	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	445
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	444
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	443
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	435
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	433
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	426
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	423
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	405
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	389
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	382
185.26.182.33	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	379
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	377
66.187.72.219	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	375
209.88.198.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	372
82.166.183.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	350

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.144.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	466
2.54.150.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	417
77.127.227.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	352
185.32.178.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	338
46.120.131.173	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.131.173	Block	280
2.54.146.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	251
37.26.147.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	232
109.253.132.192	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.132.192	Block	185
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	160
109.253.136.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
176.12.146.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
2.54.13.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
46.19.86.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.221	Block	74
109.253.130.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
176.12.150.168	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.150.168	Block	64
109.253.149.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
46.19.85.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
37.26.147.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	42
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	42
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	38
46.120.199.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
37.26.146.141	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.141	Block	36
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	34
46.19.85.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
109.253.134.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
176.12.145.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
109.253.135.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
176.12.141.120	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.141.120	Block	15
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	14
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	12
200.53.156.230	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
81.218.74.164	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.74.164	Block	11
212.25.102.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.102.63	Block	10
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	10
79.182.13.204	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	10
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	9
46.19.86.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
132.66.237.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
212.179.243.55	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 212.179.243.55	Block	8
200.53.156.180	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
176.12.151.74	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
82.166.247.98	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.166.247.98	Block	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	7
109.67.141.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
118.123.11.45	China	147.237.77.74	law.idf.il	Multiple Admin Blocking from 118.123.11.45	Block	7