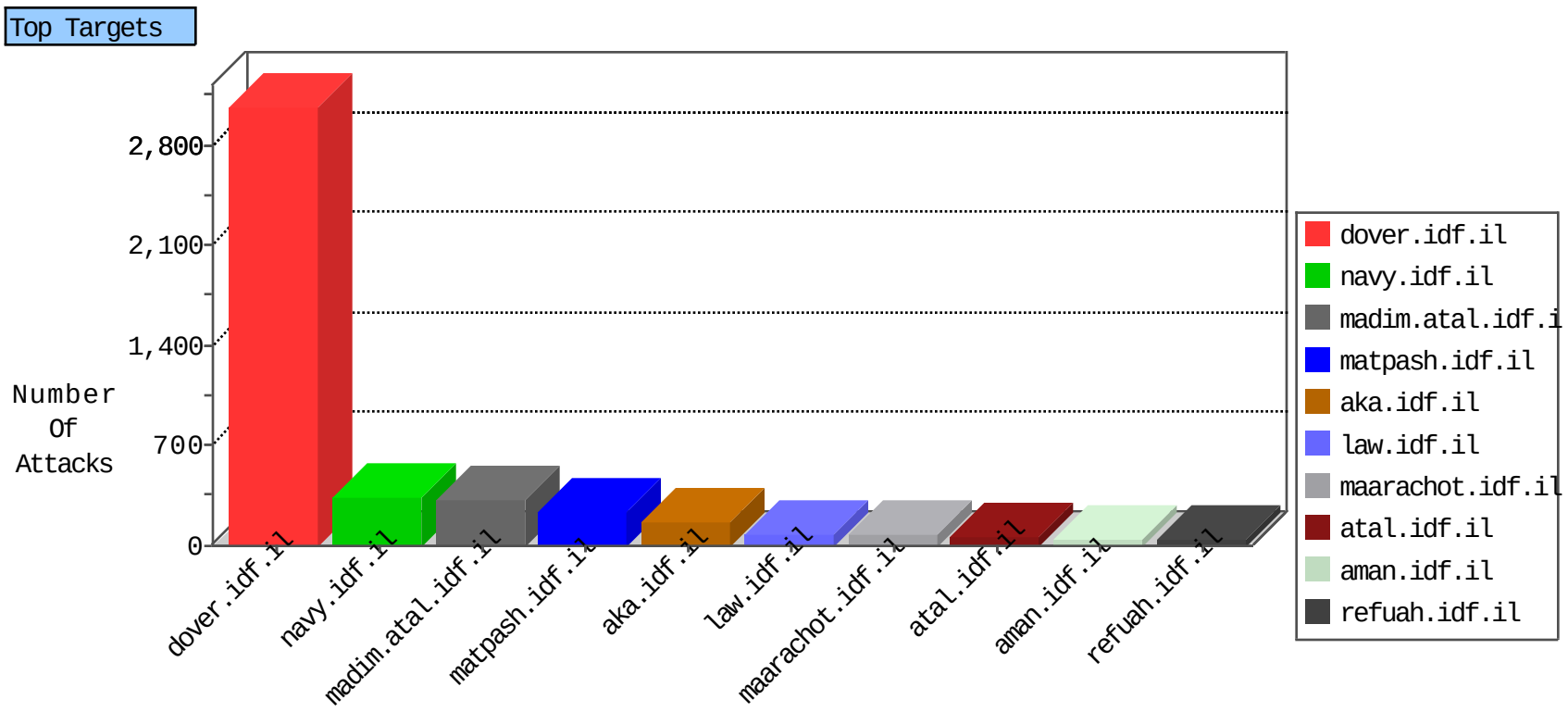
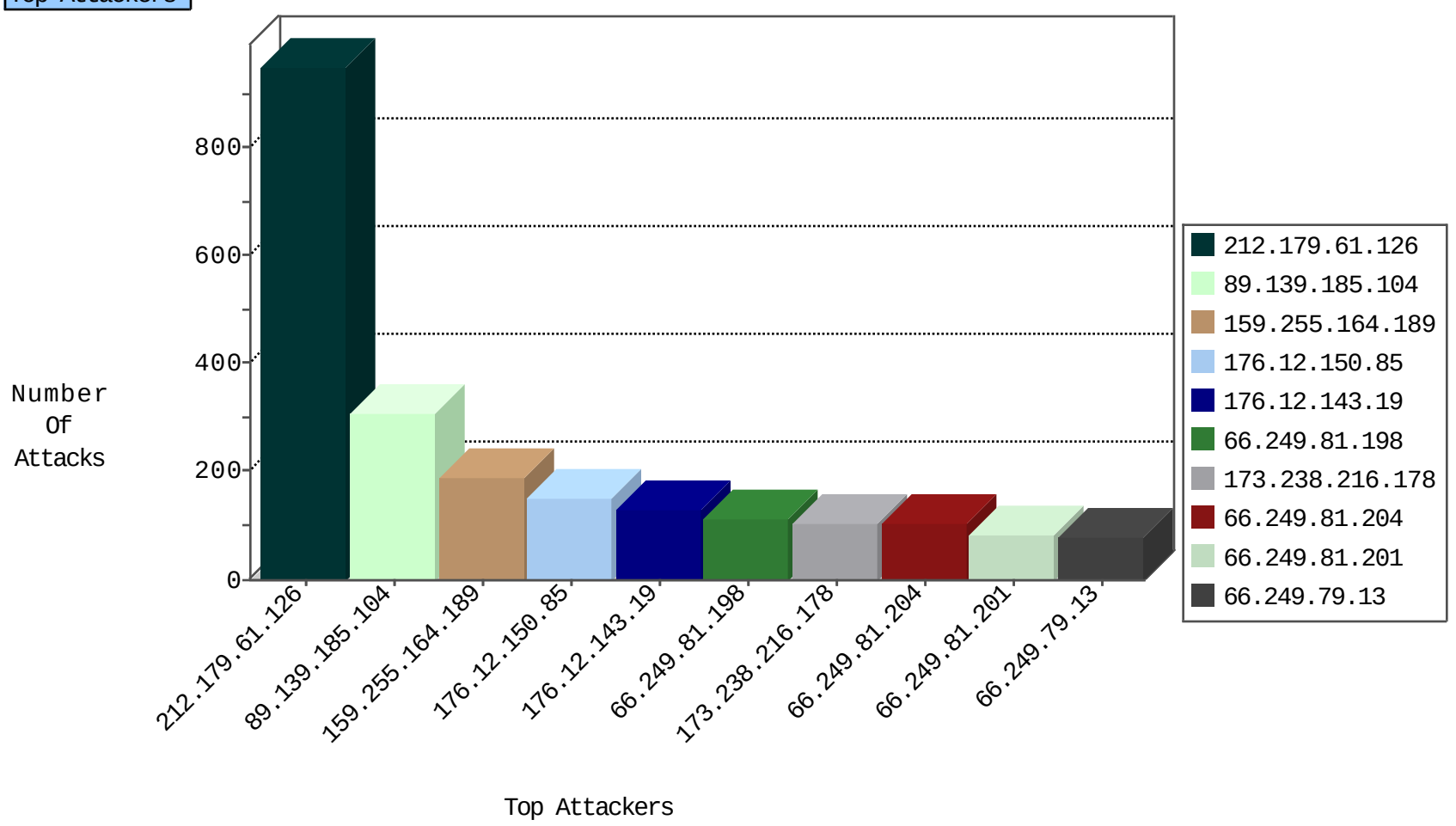
04-07-2015-19:03:06 to 04-07-2015-20:03:06

IDF Under Attack
04-07-2015-19:03:06

Top Targets



Top Attackers



04-07-2015-19:03:06 to 04-07-2015-20:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3006
84.121.189.113	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1300
46.19.85.234	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	225
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
66.249.81.198	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	111
66.249.81.204	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	104
66.249.81.201	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	83
66.249.79.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	79
66.249.79.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	75
66.249.79.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	70
93.172.38.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	25
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	25
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	20
83.40.7.106	Spain	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	15
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.69.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.67.151	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.67.159	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.81.218	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.81.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
79.179.189.28	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6

04-07-2015-19:03:06 to 04-07-2015-20:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
41.236.147.214	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.64.36.147	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
87.68.165.59	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.246.138.90	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1

04-07-2015-19:03:06 to 04-07-2015-20:03:06

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	6
46.116.232.236	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.186.34.242	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.242	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.168	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
141.212.122.88	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
59.41.39.125	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
222.186.34.242	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
43.255.191.168	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.2.101.170	Germany	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
109.253.137.37	Israel	147.237.72.166	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
43.255.191.168	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
59.41.39.125	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
58.20.54.249	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1

04-07-2015-19:03:06 to 04-07-2015-20:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	951
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	309
159.255.164.189	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	189
173.238.216.178	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
46.19.86.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
46.19.85.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
197.231.18.195	Mauritania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
176.12.147.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
79.180.221.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
173.238.216.178	Canada	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
168.63.139.43	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
186.155.252.90	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
85.250.174.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
87.208.20.67	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
2.54.6.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
76.11.116.193	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
176.12.140.60	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
217.132.112.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
24.15.165.189	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
41.109.192.57	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.85.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
77.125.115.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
41.109.147.223	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
207.250.75.253	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
81.218.50.131	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
77.127.130.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
80.40.134.104	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
41.37.148.126	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
2.52.158.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.19.85.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
212.235.35.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
82.166.85.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.210.186.136	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	8
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
98.118.10.246	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.19.85.175	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	7
84.121.189.113	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
111.93.235.58	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
79.179.106.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
213.57.31.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
77.125.125.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
89.139.59.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
132.64.30.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.150.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
176.12.143.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	129
79.181.131.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	30
176.12.146.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
87.69.162.117	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	4
176.12.143.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
176.12.139.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
31.168.170.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
84.228.255.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.138.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
46.116.144.98	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.116.144.98	Block	2
176.12.139.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
37.60.40.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
109.160.235.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
27.106.84.42	India	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on //tmunblock.cgi	Block	1
134.249.53.36	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
212.106.65.117	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
37.26.148.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
5.11.45.246	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-ar	Block	1
109.253.133.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
79.179.34.99	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/11â€‹33-19857-hâ€‹e/dover.asâ€‹px	Block	1
147.236.33.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
27.106.84.42	India	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on //tmunblock.cgi	Block	1
84.229.155.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
213.57.198.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
64.111.115.35	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
5.79.16.135	United Kingdom	147.237.76.86	navy.idf.il	Multiple signatures from 5.79.16.135	Block	1
109.253.158.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.164.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.116.144.98	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/6_s3_	Block	1
155.94.254.133		147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
31.168.170.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.170.190	Block	1
68.180.228.224	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.60.40.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
5.79.16.135	United Kingdom	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
114.112.90.54	China	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	1
46.116.144.98	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.116.144.98	Block	1
188.40.52.150	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
90.146.4.162	Austria	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
37.237.9.132	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
27.106.84.42	India	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on //tmunblock.cgi	Block	1
134.249.53.36	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
27.106.84.42	India	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on //tmunblock.cgi	Block	1
134.249.53.36	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
84.108.130.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/homefront1.stm	Block	1
46.116.144.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/6_s3_	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	1