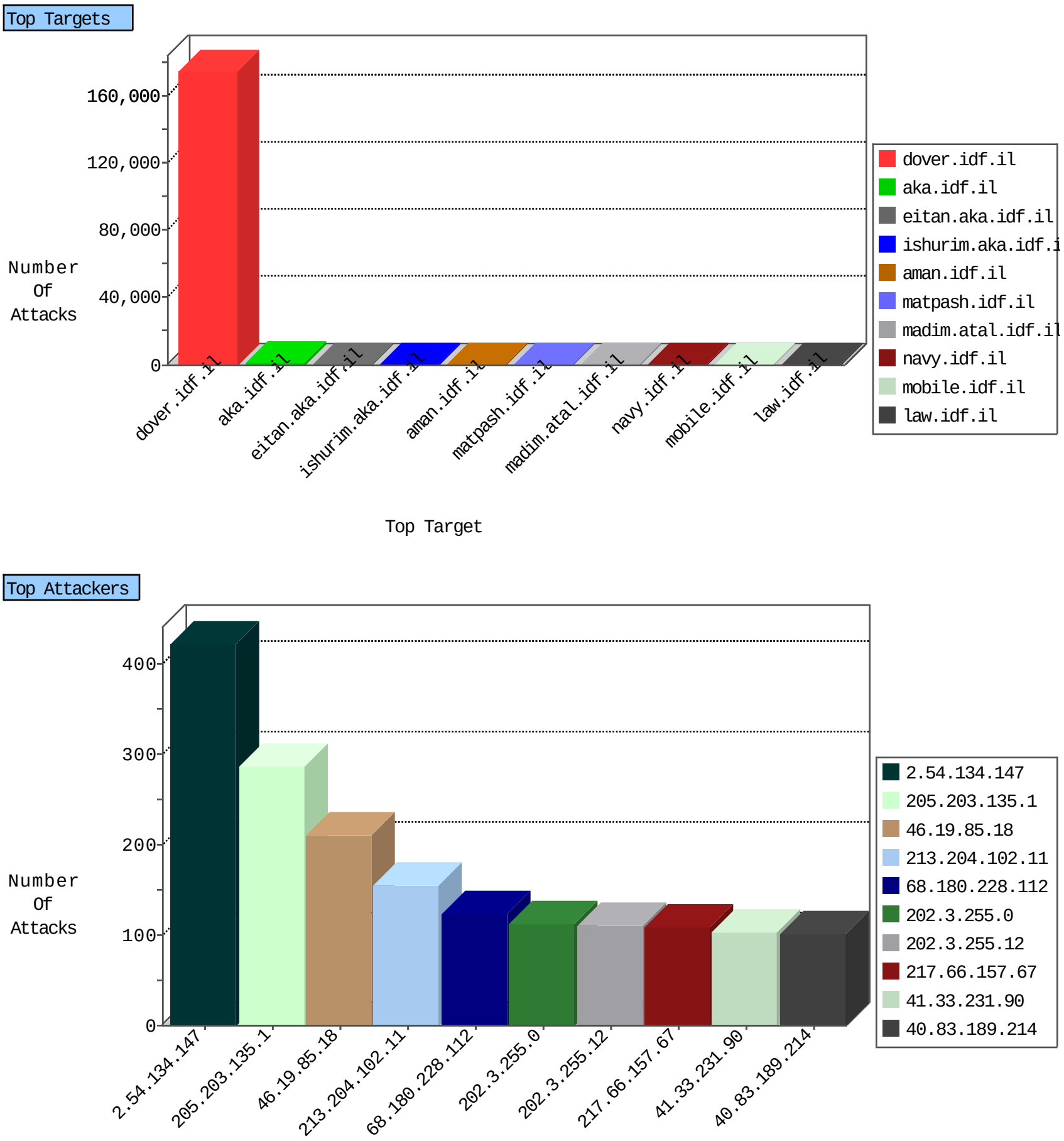
11-12-2015-19:04:09 to 11-12-2015-20:04:09

IDF Under Attack Daily Report



11-12-2015-19:04:09 to 11-12-2015-20:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.0.12.174	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4577
200.223.103.58	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3066
117.207.238.19	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2950
120.195.210.59	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2895
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	994
175.214.110.120	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	407
5.108.136.61	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	267
203.41.219.45	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	248
103.242.113.11	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	239
171.8.169.78	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	197
166.62.197.78	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	194
186.92.247.51	Venezuela	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	190
120.193.100.101	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	174
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	170
139.208.210.35	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	146
117.57.218.43	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	99
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	93
126.88.3.17	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	60
200.74.79.35	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	52
60.199.212.45	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25
77.127.60.124	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
84.229.29.97	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
192.168.34.79		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	11
132.66.10.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
192.168.1.102		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
205.203.135.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
5.102.254.51	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.177.170.134	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
187.109.19.4	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
31.208.87.83	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
213.57.235.254	Israel	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	3
82.107.203.64	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
94.245.34.101	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
42.203.63.101	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
216.173.161.59	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
207.7.74.108	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
67.6.19.51	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
93.172.151.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
24.16.196.2	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.77.190.92	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.91.242.19	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.23.247.31	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
63.248.209.10	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.133.9	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
162.220.151.23	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
219.127.237.80	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.81.239.26	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
110.20.176.1	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-12-2015-19:04:09 to 11-12-2015-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.233	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	5
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.202	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1
189.122.106.148	Brazil	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.65.73.203	Israel	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	1

11-12-2015-19:04:09 to 11-12-2015-20:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-12-2015-19:04:09 to 11-12-2015-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.134.147	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	393
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	284
46.19.85.18	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	174
213.204.102.11	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
217.66.157.67	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
40.83.189.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
71.99.166.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
129.42.208.179	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	71
37.26.148.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
106.76.234.40	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
62.210.181.90	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
67.86.213.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
52.0.238.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
91.65.212.5	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
96.49.8.107	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
208.54.70.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
99.237.119.136	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
100.100.49.31		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
207.46.13.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
52.29.121.179	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
70.199.166.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
207.46.13.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
109.65.215.9	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
105.192.186.81	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	28
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.63.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
46.19.86.81	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
207.46.13.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
52.29.135.221	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.164.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
2.54.134.147	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
95.86.116.31	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.116.31	Block	11
84.94.85.123	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/himush	Block	4
37.46.39.40	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	3
77.127.174.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.11.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.183.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.137.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.70	Block	2
75.82.54.243	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
37.46.39.40	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.46.39.40	Block	2
95.86.99.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20207-he/dover.aspx&sa=u&ved=0cakqfjaaahukewix07hetovjahwkoxqkhvf-alk&usg=afqjcnhtryxgio9uiefyzaoy9k0bdjboyq	Block	2
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.70	Block	2
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.70	Block	2
213.57.158.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.139.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.23.183	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
37.26.149.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.76	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.153.168	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
95.86.88.109	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.116.99.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.235.254	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.228.36.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.135.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.223.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.243	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;sOrderBy in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
5.29.177.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.111.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.37.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.201.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
185.32.179.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.166.22.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.76	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.76	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.95.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
46.117.38.131	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
84.228.220.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.183.180.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.139.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
132.66.236.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.94.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1