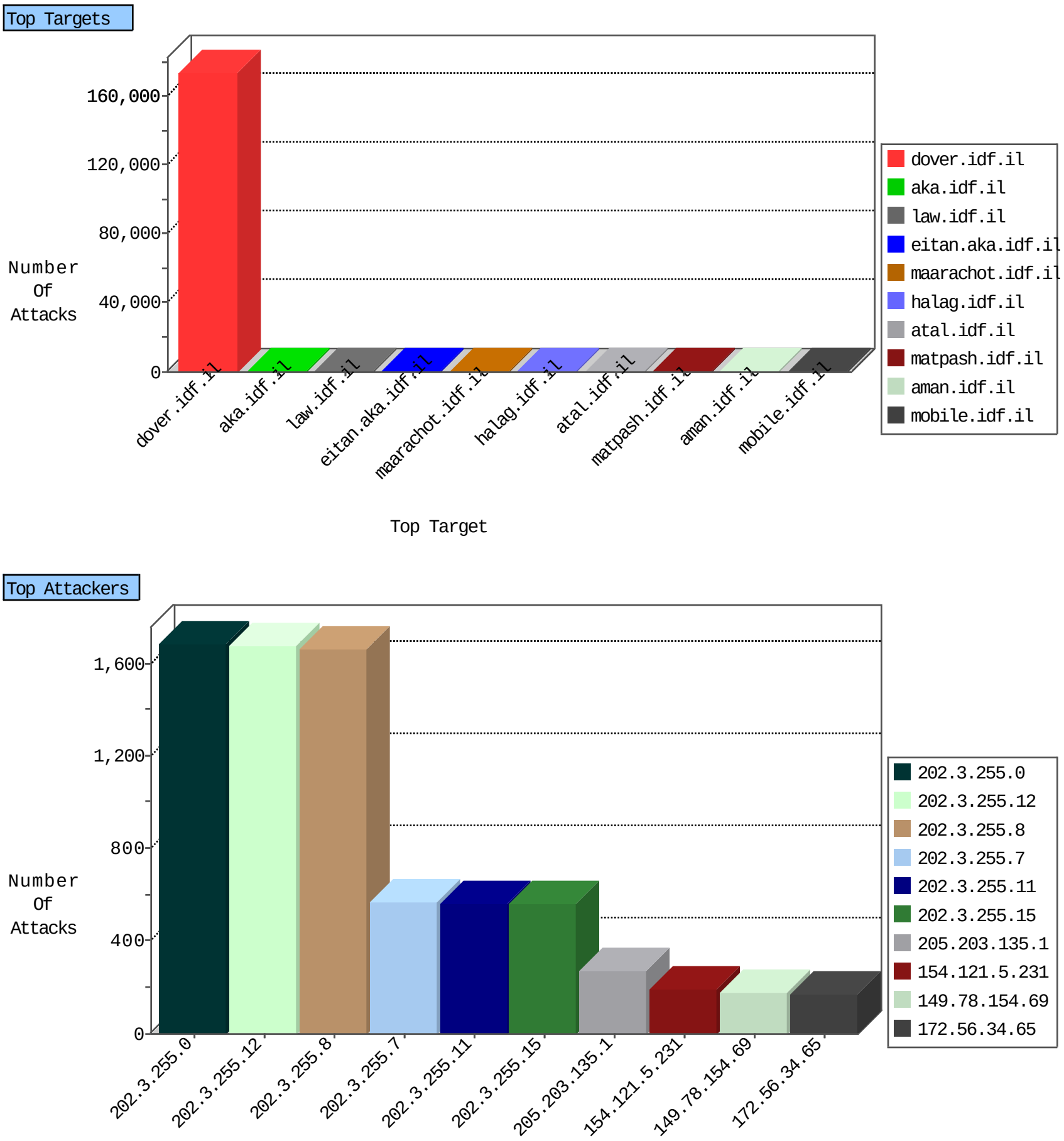
11-11-2015-04:04:06 to 11-11-2015-05:04:06

IDF Under Attack Daily Report



11-11-2015-04:04:06 to 11-11-2015-05:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.117.56.106	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3123
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	776
120.204.174.43	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	382
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	165
94.144.50.42	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	89
46.19.86.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	70
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	58
70.26.59.88	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
37.142.131.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
173.70.41.24	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.229.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
76.30.159.154	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
78.9.52.53	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
204.42.253.2	United States	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1
67.58.161.14	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
135.23.70.42	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
1.214.242.42	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.189.54.124	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.249.84	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.54.30.101	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.114.189.44	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
125.40.196.117	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
108.20.229.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.78.213.9	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.74.40.82	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
73.178.155.48	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
94.135.215.36	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
217.12.202.110	Ukraine	147.237.76.177	ncore.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1
24.178.190.39	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
90.185.157.102	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.68.48.38	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.60.243.74	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
150.162.156.116	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.185.214.4	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.112.188.56	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.21.216.41	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.2.68.72	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.45.107	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
189.205.20.6	Mexico	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.6.102	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
117.200.248.75	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
45.50.85.85		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
99.23.232.53	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.171.25.64	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
176.51.79.92	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
72.42.84.121	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
164.67.24.24	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.44.89.36	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.81.66.78	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-11-2015-04:04:06 to 11-11-2015-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.130	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	16
188.165.15.212	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	10
62.210.113.143	France	147.237.77.170	maarachot.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	5
151.80.31.125	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	5
188.165.15.36	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.114	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.14	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.32	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-11-2015-04:04:06 to 11-11-2015-05:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.0	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1572
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1569
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1553
202.3.255.7	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	532
202.3.255.11	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	526
202.3.255.15	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	524
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
204.93.154.216	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
46.19.86.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
170.106.210.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.159.118	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.110.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.117.83.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.64	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.236.77	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.201.42	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.147.64	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.21.18	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.48.121	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
186.15.60.102	147.237.77.216	Costa Rica	dover.idf.il	ET DROP Dshield Block Listed Source	1
136.228.48.127	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.229.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.174.28.59	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.66.56	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.127.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
14.215.176.20	147.237.77.216	China	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
170.67.217.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.98.56.119	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.208.80	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.162.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.233.172.155	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
201.71.5.51	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.19.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.71.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
116.197.156.46	147.237.77.216	Japan	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.82.119	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.76.54	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.156.195.189	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.154.127	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.200.79.90	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.195.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.223.25	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.242.31	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.235.99	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.178.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.112.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.50.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.181.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-11-2015-04:04:06 to 11-11-2015-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	269
154.121.5.231	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	193
172.56.34.65	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	173
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	164
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	114
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	113
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	113
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	112
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	111
72.26.31.109	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	97
52.33.66.29	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	94
2.54.132.195	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	89
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	75
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	75
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
24.214.201.114	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
91.228.127.198	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	65
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
46.19.86.3	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	61
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	61
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
110.26.211.15	Taiwan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
81.218.235.10	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
46.19.85.78	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
37.26.146.200	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
207.46.13.107	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
77.125.95.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
180.190.66.95	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
207.46.13.76	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
207.46.13.169	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
99.45.73.224	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
157.55.39.35	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
167.206.228.210	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
158.69.2.151	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	24
66.249.88.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
66.249.88.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22

11-11-2015-04:04:06 to 11-11-2015-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
46.120.174.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.8	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
77.125.133.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.35	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
104.243.24.177		147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
14.215.176.20	China	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.35	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71559.pdf	Block	1
207.46.13.10	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/	Block	1
104.243.24.177		147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
14.215.176.20	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
159.203.140.153	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
207.46.13.142	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.35	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.35	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.8	Block	1
159.203.140.153	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /	Block	1
104.243.24.177		147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2424.jpg	Block	1
159.203.140.153	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
104.243.24.177		147.237.77.74	law.idf.il	eMail Hoarding	Block	1
14.215.176.20	China	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 14.215.176.20 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
157.55.39.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mpm/neot_yuvalim.asp	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

11-11-2015-04:04:06 to 11-11-2015-05:04:06