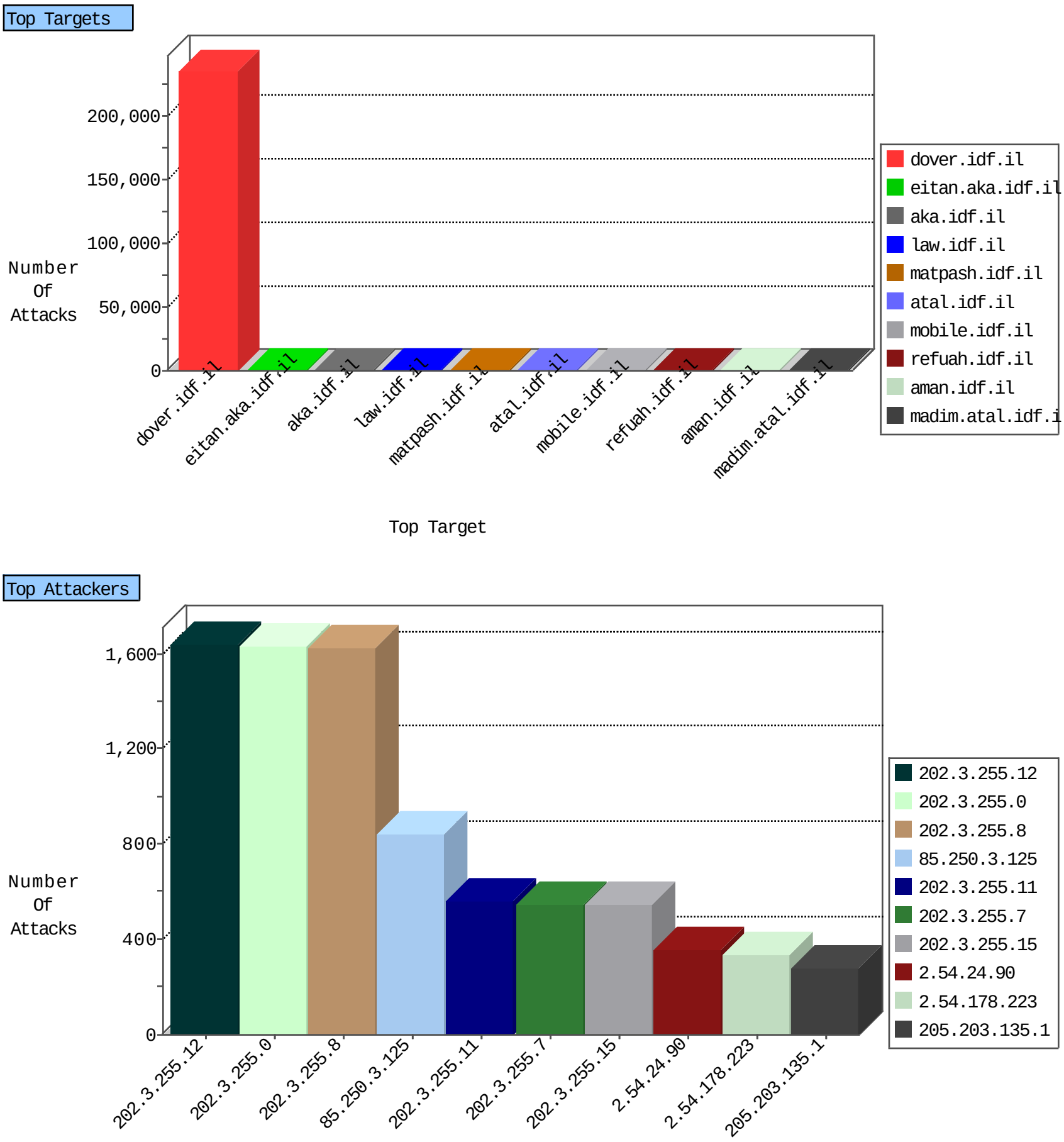
11-11-2015-06:04:02 to 11-11-2015-07:04:02

IDF Under Attack
Daily Report



11-11-2015-06:04:02 to 11-11-2015-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4661
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4571
66.249.93.200	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3450
66.249.78.79	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3400
140.122.2.85	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3359
119.194.58.44	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3227
126.141.51.44	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3202
222.177.160.123	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3069
189.98.15.24	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3035
207.46.13.169	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3016
61.138.203.89	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2944
120.179.157.90	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2516
64.206.154.254	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2434
112.140.219.1	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	586
93.91.220.95	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	519
179.149.152.124	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	481
180.168.124.1	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	340
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	288
126.91.84.118	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	270
123.21.100.79	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	249
220.94.17.57	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	230
188.138.9.49	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	218
126.78.14.11	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	177
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	174
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	168
12.104.128.25	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	157
1.249.20.113	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	117
101.22.122.2	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	112
36.39.89.38	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	95
125.11.70.34	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	88
126.238.75.70	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	82
124.54.188.79	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	64
45.216.202.46	Uruguay	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	61
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	58
167.60.23.90	Uruguay	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	58
220.181.108.146	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	47
117.205.176.61	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42
126.4.7.48	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
59.34.6.43	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34
92.232.238.12	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31
85.250.208.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
79.180.99.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
36.229.80.113	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
176.13.8.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
120.176.193.41	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
79.183.107.111	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
2.54.153.31	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
108.56.75.138	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7

11-11-2015-06:04:02 to 11-11-2015-07:04:02

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	15
188.165.15.212	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	8
188.165.15.14	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.202	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.202	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.85	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
193.254.206.6	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
151.80.31.125	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.129	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-11-2015-06:04:02 to 11-11-2015-07:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1530
202.3.255.0	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1519
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1518
202.3.255.11	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	521
202.3.255.7	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	507
202.3.255.15	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	506
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.64.197	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
176.47.243.2	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.168.16	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.182.95.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.203.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
77.127.29.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.167.185.125	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.157.4	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
108.161.151.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
129.76.126.42	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.182.90.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.94.14	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.90.73	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.245.138.67	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.130.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.188.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.190.9	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.227.83.122	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.145.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.84.39	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.241.102	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
129.76.87.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.83.102	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.111.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.31.18	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.33.145.18	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.64.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.134.64	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
50.204.188.142	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
170.113.25.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.205.89	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.23.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.144.54	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.151.116.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.83.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.244.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.85.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
128.168.199.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.144.191.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.12.101	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.88.59	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-11-2015-06:04:02 to 11-11-2015-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.24.90	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	342
2.54.178.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	335
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	278
192.0.81.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	211
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	191
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	134
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
104.33.203.232	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
47.88.13.149	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
202.3.255.8	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	111
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
174.115.28.30	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
2.54.175.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
64.206.154.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.4.110.30	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.13.8.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.13.21.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.13.23.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
2.54.153.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.15	French Polynesia	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
207.46.13.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.102.7.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
108.56.75.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
84.110.81.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.117.57.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
213.57.54.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.13.0.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29

11-11-2015-06:04:02 to 11-11-2015-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	780
176.31.126.56	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.31.126.56	Block	9
2.54.24.90	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.24.90	Block	9
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
176.12.145.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.104.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
14.215.176.20	China	147.237.77.233	atal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
14.215.176.21	China	147.237.77.233	atal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
85.64.202.120	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.11.41	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.131	Block	1
176.31.126.56	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/shared/usercontrols/headerupper/	Block	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69739.pdf	Block	1
204.236.235.245	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
14.215.176.149	China	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.24.90	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
207.46.13.75	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
14.215.176.149	China	147.237.77.233	atal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
217.31.48.30	Czech Republic	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/rom-0	Block	1
85.65.157.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
47.88.13.149	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/forum/ajax/api/hook/decodearguments	Block	1

11-11-2015-06:04:02 to 11-11-2015-07:04:02