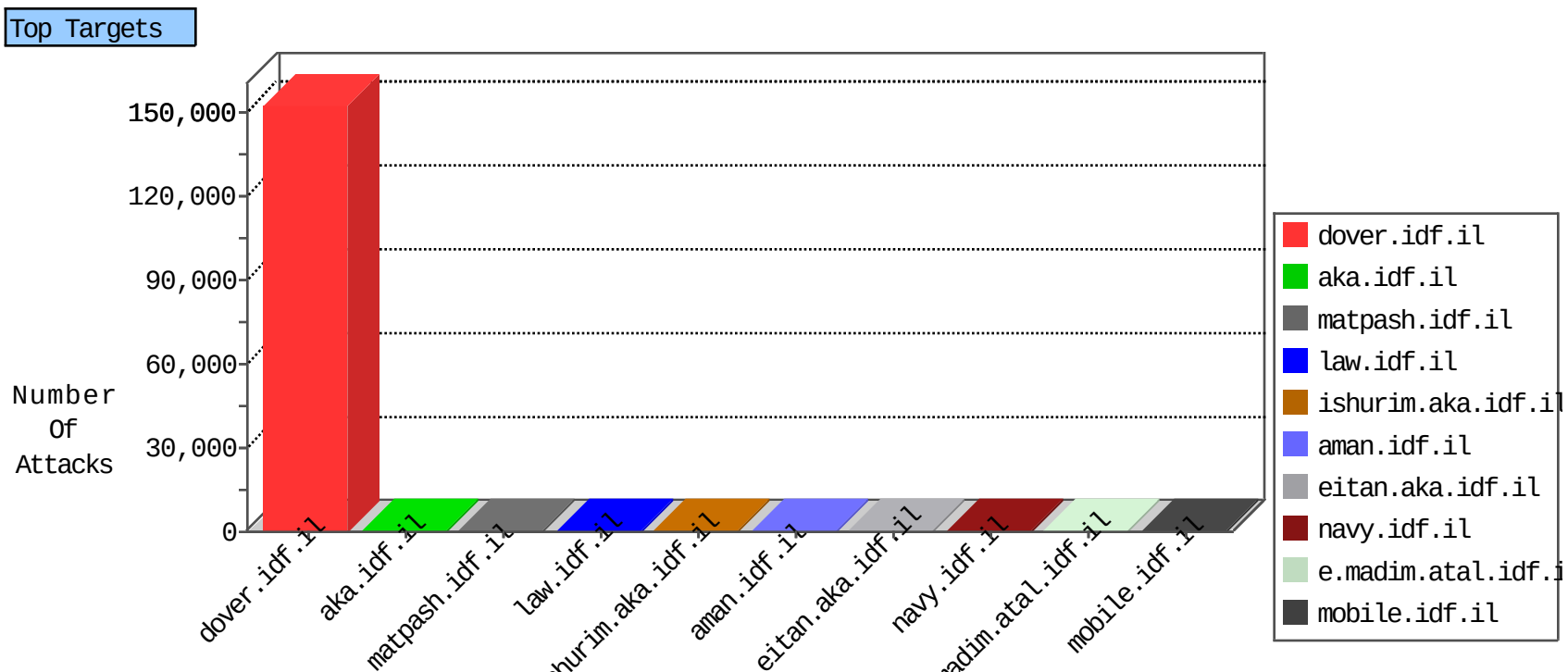
11-13-2015-05:04:08 to 11-13-2015-06:04:08

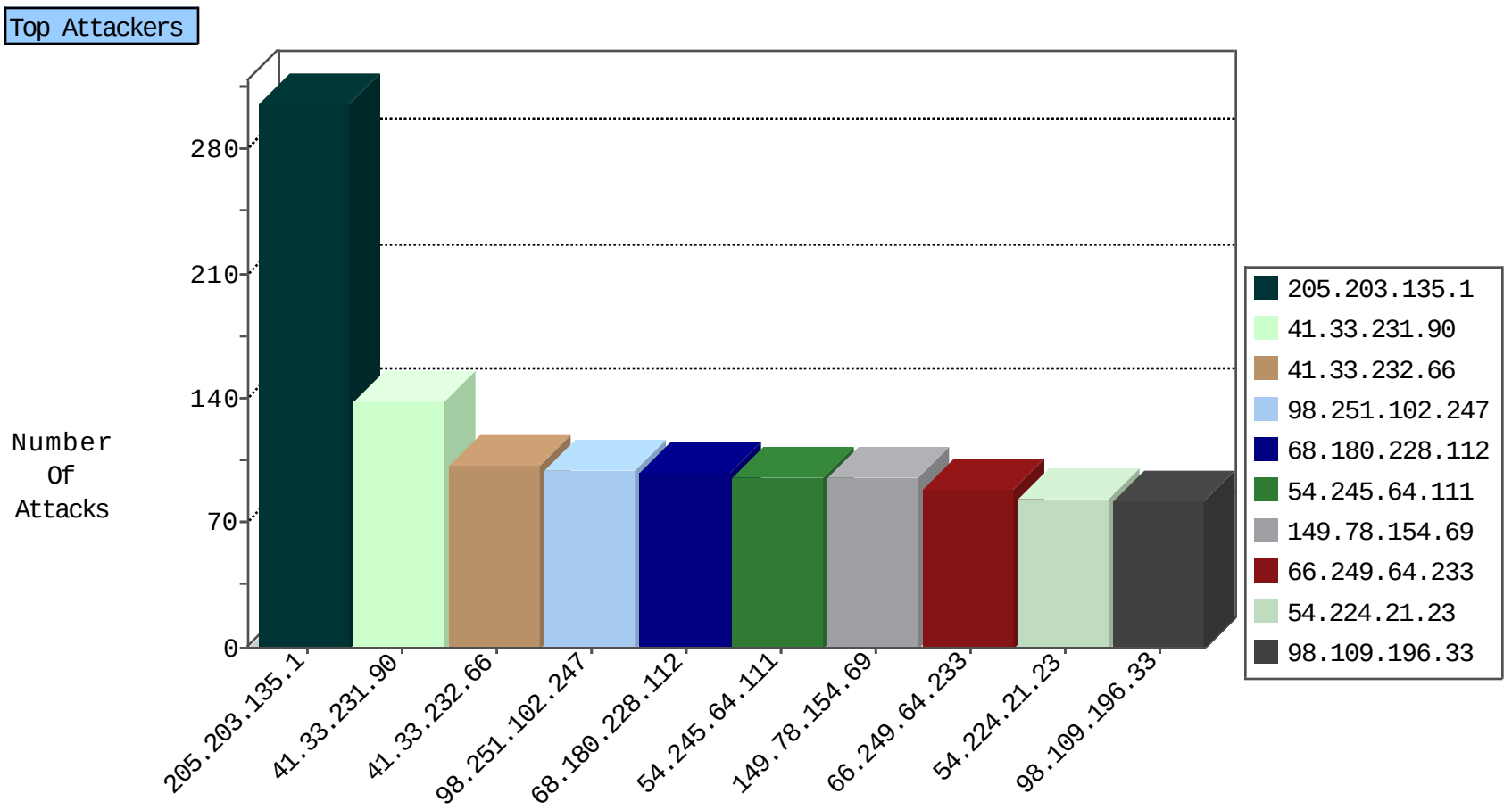
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-13-2015-05:04:08 to 11-13-2015-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.38.101.16	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3115
107.171.165.98	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3074
202.21.163.14	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2990
123.108.167.33	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2795
181.26.181.69	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2777
125.161.102.2	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2760
180.68.168.42	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2692
5.196.177.74	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2609
112.173.151.102	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2595
111.50.88.44	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	622
176.216.224.3	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	591
150.49.15.36	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	432
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	410
179.126.71.47	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	352
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	189
168.1.30.88	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	188
218.157.85.113	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	151
175.162.251.72	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	147
134.115.74.25	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	145
92.127.254.58	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	132
189.227.242.30	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	122
201.250.247.64	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	120
64.86.115.21	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	111
119.168.11.122	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	102
14.100.23.80	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	101
176.54.117.127	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
171.89.56.32	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
87.241.132.61	Armenia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	87
221.184.192.45	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	87
110.131.199.59	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	75
119.213.42.54	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	75
179.8.134.39	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	75
114.254.164.32	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	60
171.77.216.2	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
114.27.179.117	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	8
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
193.34.70.8	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
85.19.222.78	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
217.112.34.50	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
36.97.52.94	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
170.110.236.97	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.75.118.83	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.31.244.17	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
116.12.134.116	Singapore	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.20.60.77	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
67.191.77.100	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
188.112.106.96	Slovakia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.148.123.50	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
87.18.153.111	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-13-2015-05:04:08 to 11-13-2015-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.201	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.131	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-13-2015-05:04:08 to 11-13-2015-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
157.232.114.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.215.140.12	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
190.220.168.6	147.237.72.167	Argentina	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
138.43.214.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.6.71.154	147.237.0.33	Poland	idf.il	ET SCAN NMAP -sS window 1024	1
170.67.153.50	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.208.45	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.101.186.178	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
143.135.235.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.69.20	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.189.5	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
190.220.168.6	147.237.72.156	Argentina	aman.idf.il	ET SCAN Potential SSH Scan	1
136.228.127.125	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.60.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.110.46	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.48.19.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.154.95	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
14.63.73.39	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
94.130.120.79	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
188.34.238.161	147.237.8.27	Iran, Islamic Republic of	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
136.228.39.14	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.138.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.146.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.113.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.33.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
14.63.73.39	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
176.47.223.107	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.20.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.189.2.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.95.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.202.206.113	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.116.38.118	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.201.192.17	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.155.121	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.106.98	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.75.61	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.242.121	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.32.158.1	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.145.89	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.68.52	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.63.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.0.126	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
116.199.142.4	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.203.225.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.226.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.106.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.56.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-13-2015-05:04:08 to 11-13-2015-06:04:08

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.il	drop	First packet isn't SYN	drop	306
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
98.251.102.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
98.109.196.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	60
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
182.64.26.61	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
207.46.13.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
104.158.24.21	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
157.55.39.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	34
52.29.142.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	27
24.113.51.195	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
67.10.163.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
207.46.13.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	23
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
172.56.26.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.80.46.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
94.98.46.152	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
207.46.13.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
199.184.236.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
88.198.157.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.46.13.120	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	19
207.46.13.23	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
108.168.121.38	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.64.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
207.46.13.24	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.146.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

11-13-2015-05:04:08 to 11-13-2015-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.222.233	Block	4
37.60.150.86	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	3
37.142.209.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.103	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	1
156.110.139.125	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
66.249.66.90	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
199.30.25.102	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter DocID in www.aka.idf.il/giyus/atuda/	None	1
40.77.167.103	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/qanda/default.asp	None	1
156.110.139.125	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
66.249.66.95	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/terms.aspx	Block	1
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
207.46.13.53	United States	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
156.110.139.125	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
40.77.167.40	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
217.31.48.13	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/rom-0	Block	1
141.212.122.80	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /x	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
157.55.39.97	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/www.rabanut-downloads.webs.com	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.103	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
156.110.139.125	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1

11-13-2015-05:04:08 to 11-13-2015-06:04:08