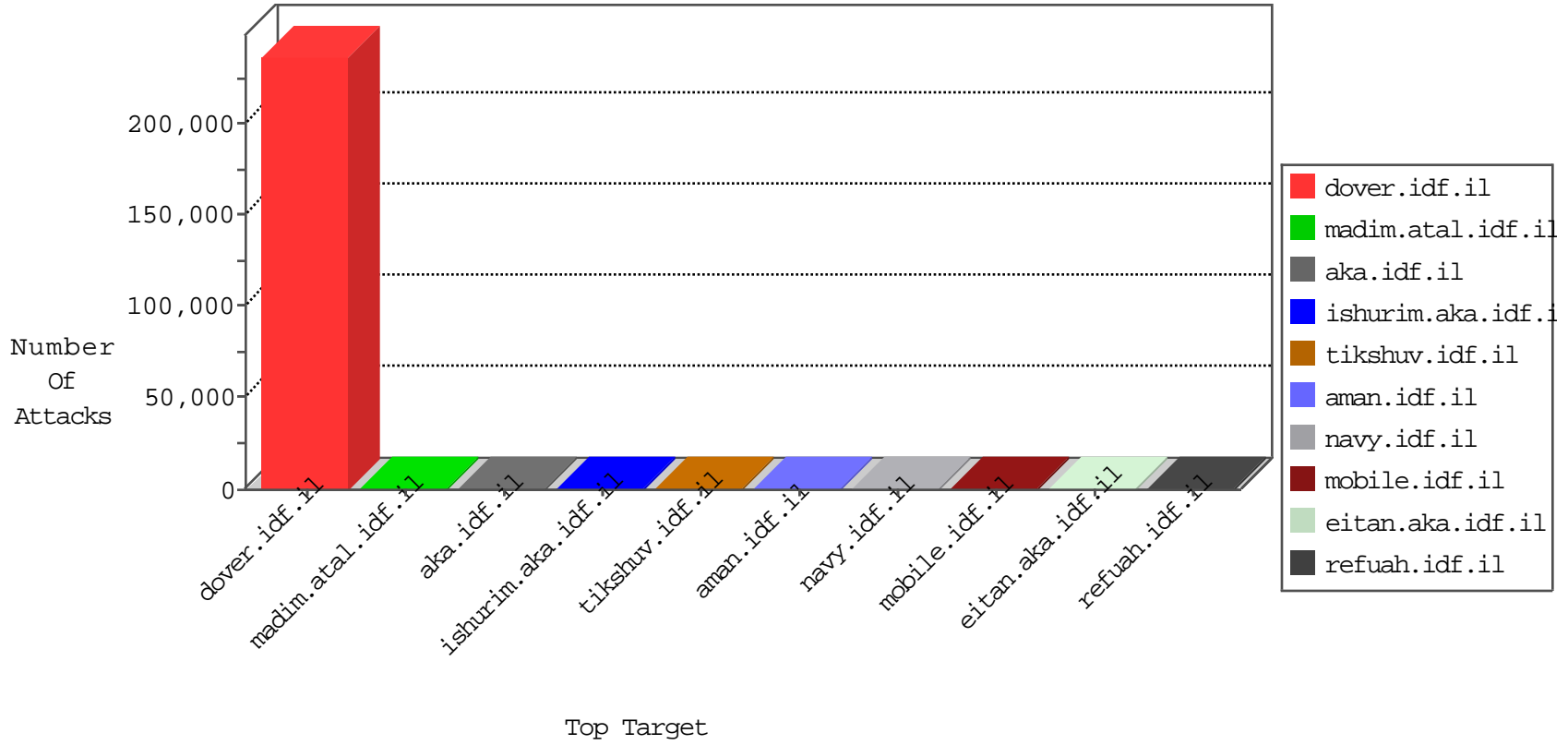


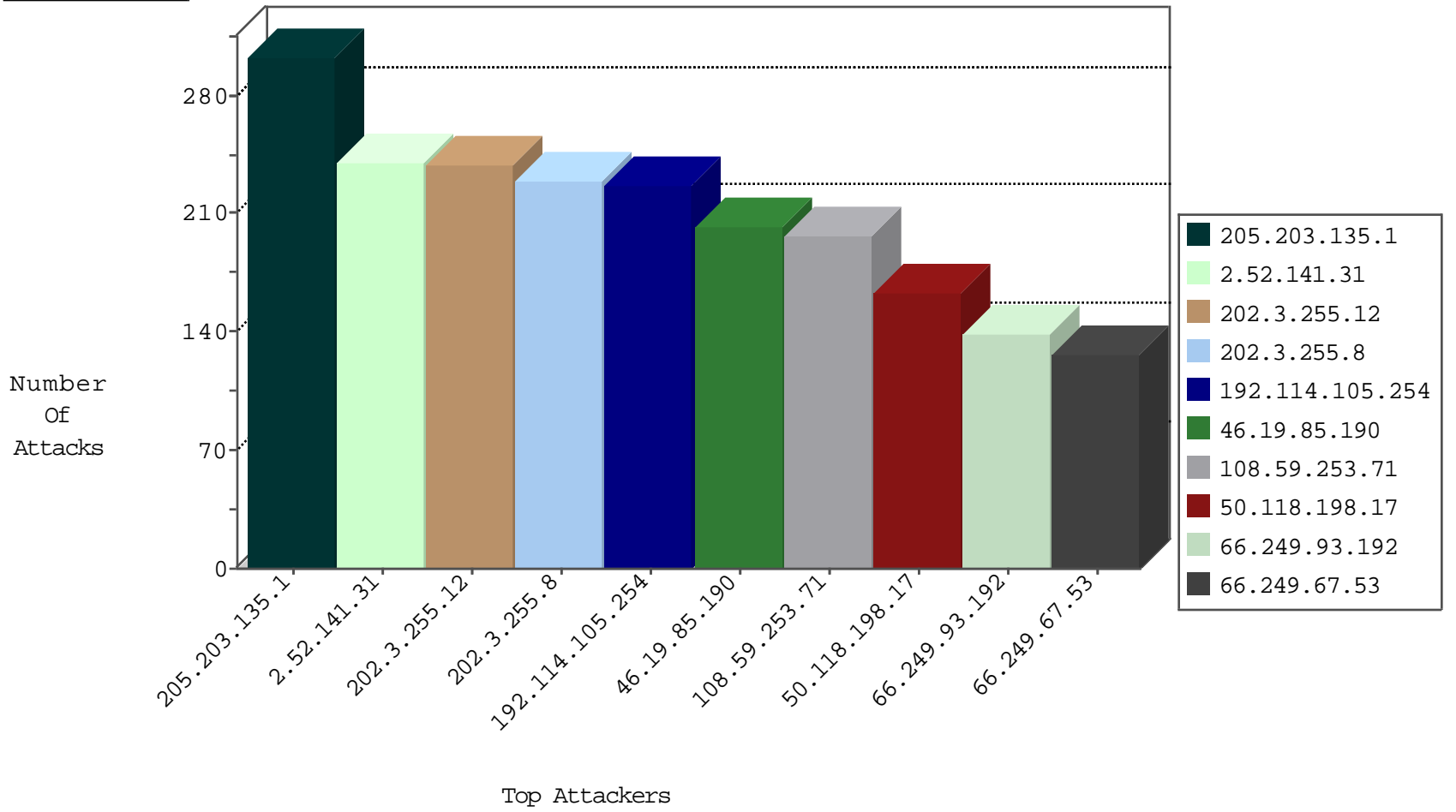
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.123.141.105	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6274
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4057
41.46.111.45	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3250
94.69.235.27	Greece	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3151
117.211.156.53	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2736
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
66.249.64.186	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	155
211.75.79.103	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	111
46.19.86.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
109.64.63.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
46.120.229.123	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
84.94.161.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
178.122.187.18	Belarus	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
88.206.203.89	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
2.142.23.126	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
188.175.149.101	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
79.182.53.196	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
93.173.144.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
155.4.80.109	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
31.168.138.81	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
63.248.83.23	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
8.26.245.56	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.58.112.113	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.222.124.96	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.140.36	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
50.177.62.57	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.245.33.86	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.170.218.89	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.248.158.13	Colombia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.91.10	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
172.97.252.95		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.209.9.107	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.148.123.67	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.239.138.34	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.168.101.66	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.189.212.70	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.192.85	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.211.237.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.80.234.84	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
98.196.251.51	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
2.54.47.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
77.107.41.127	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
72.42.105.24	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.176.82	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.217.83	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.160.59.78	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-19-2015-09:04:02 to 11-19-2015-10:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	202
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	191
134.209.210.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.34.139.34	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.68.107	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.85.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
104.34.89.87	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
157.231.84.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.189.171.92	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
193.104.153.34	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.62.52	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.32.55	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.86.69.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.219.133.86	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.63.1	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.228.248.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.47.89.94	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.215.46	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.8.46.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.227.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.3.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.50.30.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.96.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.246.130.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.97.52.25	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.99.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.147.252.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.220.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.218.212.32	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.19.29	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.90.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.184.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.20.69.98	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1
128.168.71.121	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.92.72	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
194.50.116.59	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.168.24	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.52.151.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
157.231.32.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.219.181.63	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.137.48	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.137.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -ss window 1024	1
176.47.135.26	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.151.54.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
148.178.7.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.213.175.9	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.13.9.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

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	303
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	197
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	121
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
68.231.212.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
50.118.198.17	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	94
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	80
82.113.99.168	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
37.26.146.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
85.64.235.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
79.176.62.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.86.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.19.85.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.19.85.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	40
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.67.59	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
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
77.158.88.40	France	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
50.118.198.17	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
66.249.67.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
166.137.248.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.8.38.9	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
98.234.237.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
108.168.121.38	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.13.10.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
79.182.191.228	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
37.26.146.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
69.171.148.98	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
207.46.13.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
162.243.73.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.153.46.216	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
77.158.88.41	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.12.147.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
198.251.53.48	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.141.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
192.114.105.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
62.219.154.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
192.114.105.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
176.13.7.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
2.52.141.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
2.54.152.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.16.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
192.114.105.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	24
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
132.72.163.213	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
46.19.86.86	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.86	Block	17
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
176.12.145.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.52.141.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	12
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.146.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.0.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.12.151.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.165.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.15.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.160.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.187.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.144.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.145.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.150.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.39.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.139.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.228.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.141.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.86	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
157.55.39.180	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
217.194.197.154	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
176.13.16.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.173.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	2
77.125.112.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	2
2.54.29.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.38.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2