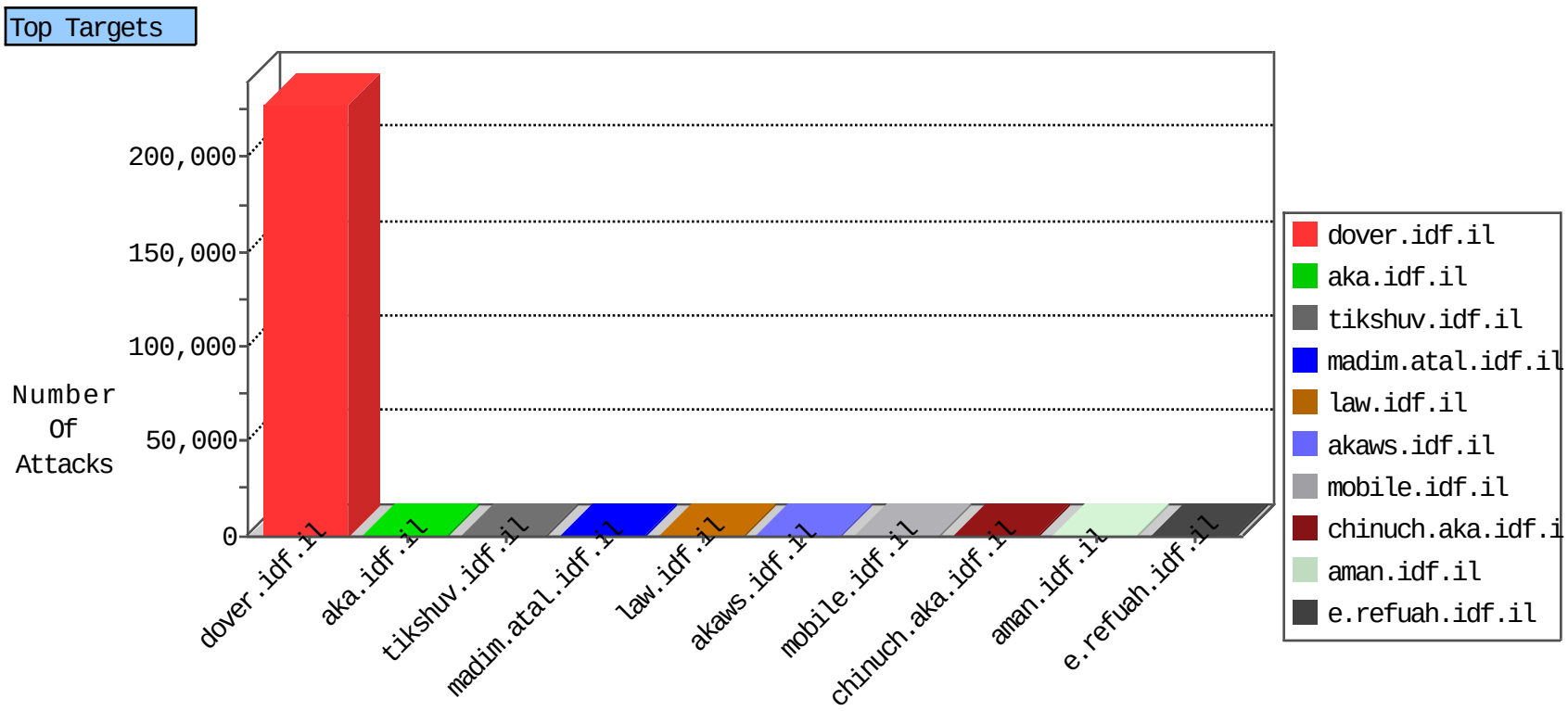
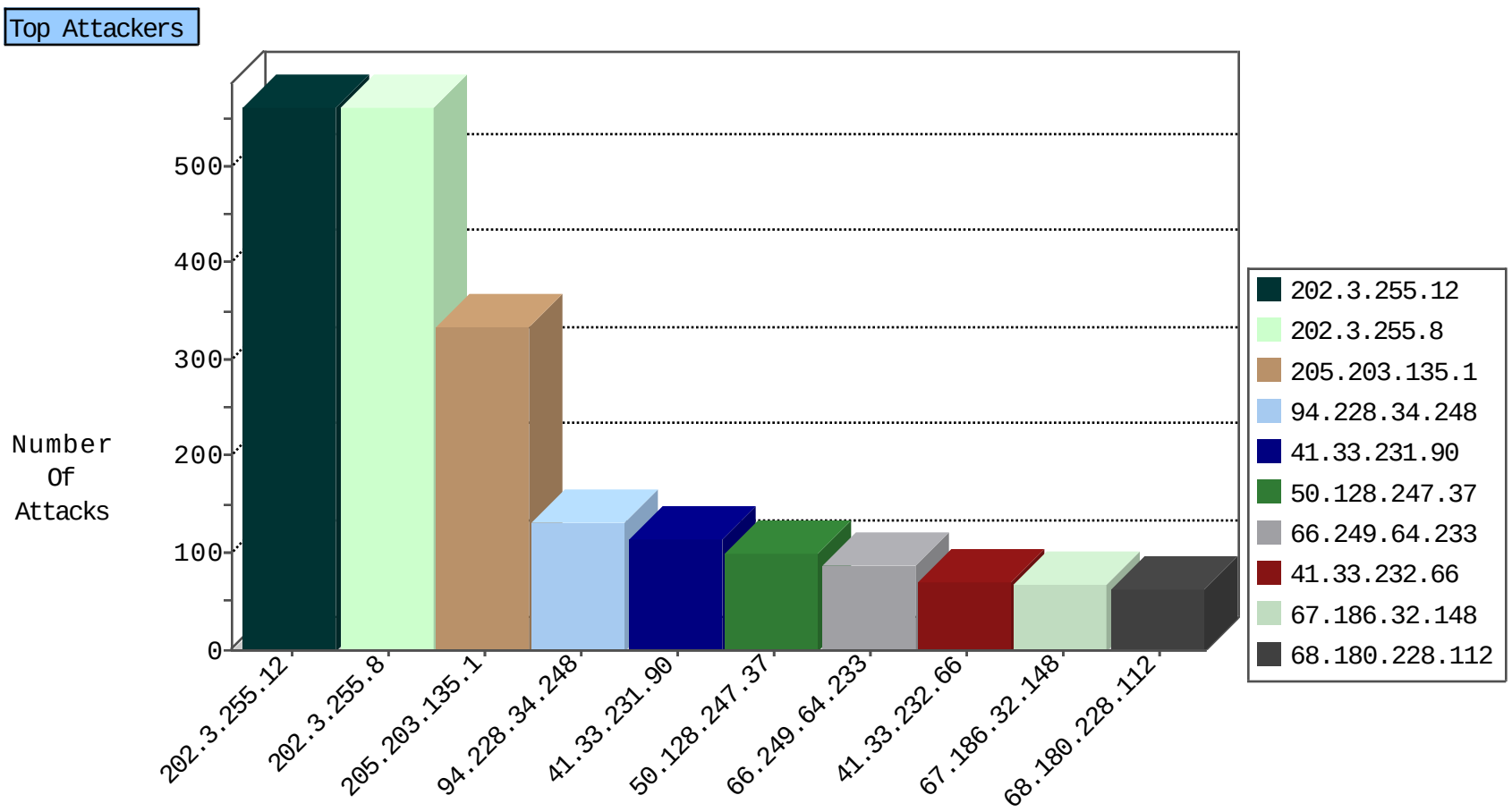
11-20-2015-02:04:00 to 11-20-2015-03:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-20-2015-02:04:00 to 11-20-2015-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.35.65.110	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	115
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
69.9.56.70	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.86.83.6	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.100.155.23	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.3.22.72	United Kingdom	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
88.146.195.65	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.218.75.81	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.138.210.47	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.237.32	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.4.105.172	United States	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
84.74.175.62	Switzerland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.235.154.126	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.173.170.51	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.176.6.66	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
109.189.242.105	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
37.157.190.61	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.201.95	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.170.212.84	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
201.187.97.26	Chile	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.225.191.79	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
182.171.64.31	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
8.30.179.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
92.26.82.28	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.100.136.29	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.234.248.88	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.238.78.39	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
134.131.69.87	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
80.253.202.36	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.102.39	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.203.185.43	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.169.36	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.53.41.3	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.31.209.7	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.169.115.95	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.243.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.124.7.112	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.233.192.24	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.114.178.108	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
175.207.241.41	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.249.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.4.105.172	United States	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Http	drop	1
84.215.105.73	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
77.95.166.5	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.238.252.60	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
119.79.58.43	China	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
42.2.124.119	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.207.121	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.170.218.46	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-20-2015-02:04:00 to 11-20-2015-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-20-2015-02:04:00 to 11-20-2015-03:04:00

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	524
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	523
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
95.216.153.99	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.11.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.176.42	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.187.226.71	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.150.104	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.30.67	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
52.16.5.197	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
140.170.127.44	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.255.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.142.81.29	147.237.76.30	Tajikistan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.168.3.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.132.20	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
24.68.10.227	147.237.76.30	Canada	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
204.44.230.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.155.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.91.29	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.93.89	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.116.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
203.34.70.24	147.237.77.216	Australia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.73.228.130	147.237.76.44	Singapore	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
170.106.141.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.82.88	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.18.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.173.57	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
108.61.173.180	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
170.67.38.114	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.89.15	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.217.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.23.34.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
101.24.83.229	147.237.0.19	China	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
147.50.116.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.18.68	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.8.24	United States	e.lifestyle.idf.	ET SCAN NMAP -sS window 1024	1
134.172.84.122	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
194.50.116.120	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
98.119.105.221	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
147.50.72.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.77.234	United States	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
130.201.181.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.238.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.107.124	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.233.96	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.170.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
130.201.22.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.139.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.250.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-20-2015-02:04:00 to 11-20-2015-03:04:00

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	335
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	132
50.128.247.37	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	100
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	76
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
67.186.32.148	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
104.169.73.179	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
107.23.6.162	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
208.80.155.255	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
88.176.18.68	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	35
83.50.184.96	Spain	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
66.249.64.230	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
107.170.63.50	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
24.79.220.59	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
178.63.165.187	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
222.163.195.6	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
157.55.39.117	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
205.197.242.155	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
66.249.64.230	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
52.68.136.185	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
69.175.127.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
205.197.242.155	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	15
24.124.59.204	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
204.93.154.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
139.162.216.112	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
157.55.39.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
176.13.7.126	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
198.1.101.123	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
128.242.249.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
88.198.25.217	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
104.129.192.116	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12

11-20-2015-02:04:00 to 11-20-2015-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.175.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.93.154.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
88.176.18.68	France	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/flash/recruitlane/recruitlane.swf	Block	1
141.8.142.4	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8859-he/refuah.aspx	Block	1
176.13.3.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19795-he/idfgdover.aspx	Block	1
79.178.51.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.93.154.216	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1

11-20-2015-02:04:00 to 11-20-2015-03:04:00