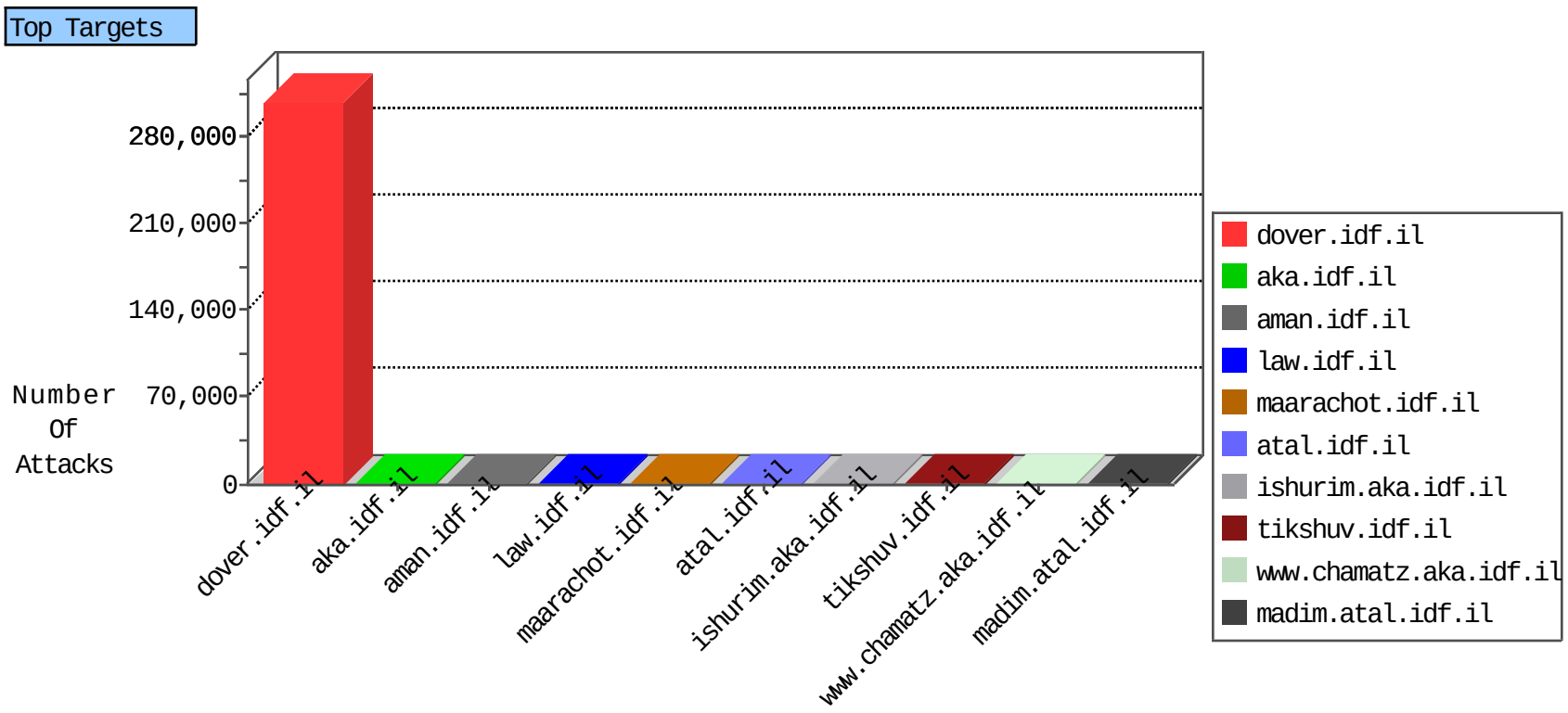
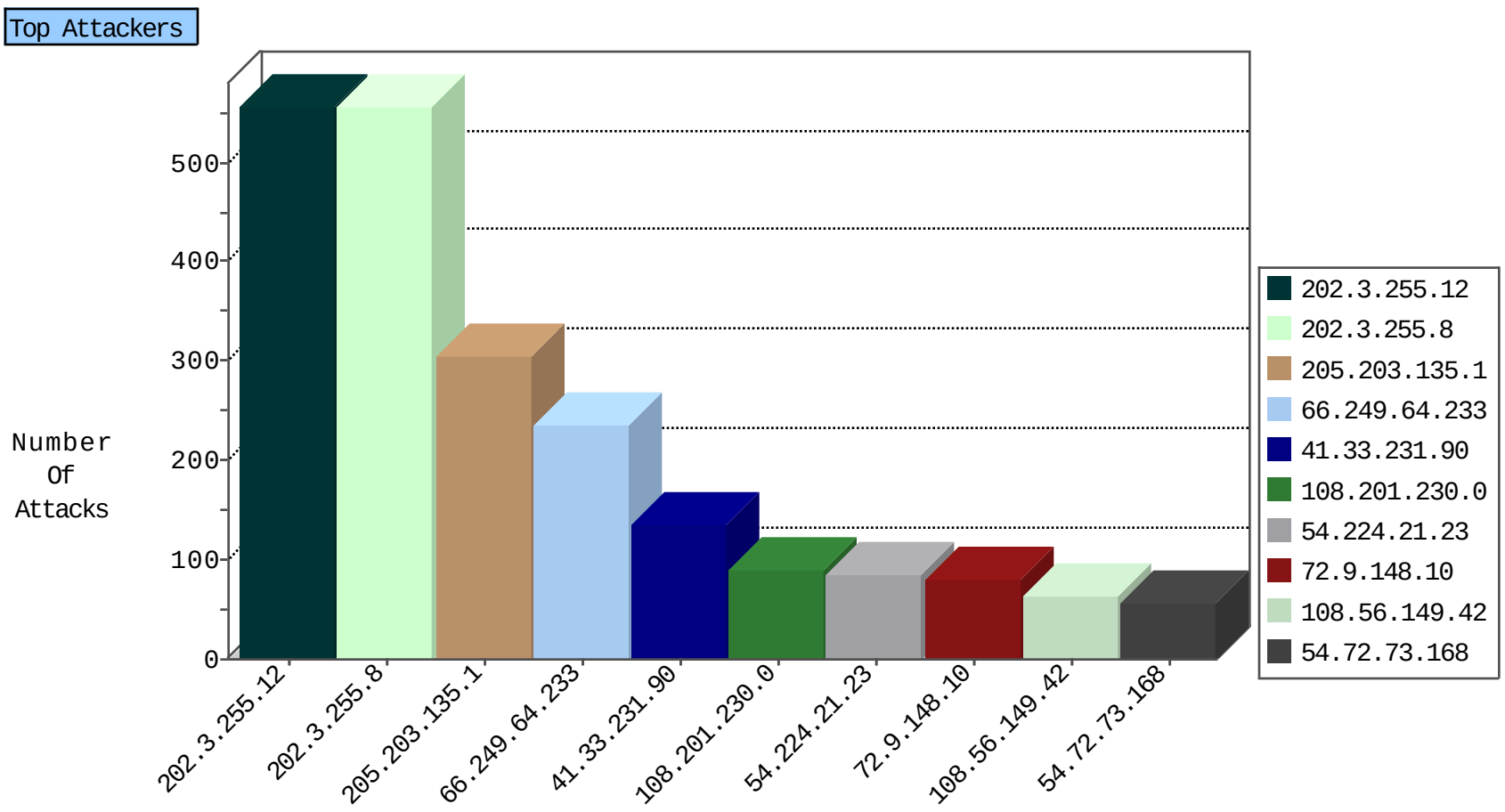
11-20-2015-01:06:18 to 11-20-2015-02:06:18

IDF Under Attack Daily Report





11-20-2015-01:06:18 to 11-20-2015-02:06:18

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.65.219.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4809
204.93.154.216	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	18
31.208.32.124	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
75.133.181.50	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
24.105.220.63	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
77.111.165.39	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.190.19.42	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.19.152.101	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
100.42.169.118	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.94.56.82	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.202.114	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.57.16.123	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
18.83.3.99	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.81.253.2	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
191.16.24.120	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
70.63.184.75	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.138.217.12	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.228.26.12	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.23.66.67		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
211.226.93.74	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.75.160.113	Switzerland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.69.212.105	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.241.73.46	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
157.158.16.120	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.218.73.20	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.197.238.105	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.148.120.34	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
79.215.5.42	Germany	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
198.100.137.92	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
23.233.81.4	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.109.140.75	Austria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.189.41	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.254.114.29	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.238.244.67	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.69.221.59	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.101.57.33	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.85.73.62	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
2.143.83.2	Spain	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
186.137.3.126	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.63.37.18	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
169.226.184.44	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.59.45.4	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.52.28.71	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.141.92	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.29.22	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
201.231.59.75	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.185.210.96	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
146.6.123.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-20-2015-01:06:18 to 11-20-2015-02:06:18

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.127	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.138	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.208	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-20-2015-01:06:18 to 11-20-2015-02:06:18

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	520
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	518
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.65.43	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.248.11.97	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.140.73	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.73.228.130	147.237.8.45	Singapore	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
150.126.116.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.110.48.114	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.151.123.110	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.130.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.34.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.141.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.108.21.16	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
207.189.23.6	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.2.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.98.23	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.151.78.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.215.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.93.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.20.162.57	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.183.195.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.73.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
149.210.216.111	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
64.112.45.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.20.69.74	147.237.77.170	United States	maarachot.idf.il	ET DROP Dshield Block Listed Source	1
134.127.49.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.42.122	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.200.157.163	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
206.227.71.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.72.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.177.39	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
130.201.181.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
149.210.216.111	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
167.97.69.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.246.117	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.144.186.72	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.121.41	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
128.199.104.102	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
149.210.216.111	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
64.44.137.39	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.11.117	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.142.107.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.174.56	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.202.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.78.122	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-20-2015-01:06:18 to 11-20-2015-02:06:18

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	306
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	160
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	107
108.201.230.0	United States	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
108.56.149.42	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
83.169.10.185	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
222.163.195.6	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
113.5.80.71	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
72.65.219.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
110.168.230.234	Thailand	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
100.100.82.99		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
66.249.64.233	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
94.249.112.190	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
157.55.39.117	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
208.180.76.24	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	23
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
54.162.150.242	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
62.128.48.130	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
204.12.251.37	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
216.113.202.149	Canada	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	20
178.63.165.187	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
62.210.250.215	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
68.196.82.74	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
181.171.218.173	Argentina	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
128.242.249.13	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
37.250.203.74	Sweden	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
204.93.154.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
157.55.39.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.26.212	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
216.113.202.149	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14

11-20-2015-01:06:18 to 11-20-2015-02:06:18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.107.79	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.4.107.79	Block	4
176.12.142.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.74.164	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.74.164	Block	3
217.132.254.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.66.131.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.181.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
77.127.133.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
141.212.122.112	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to /x	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born4.stm]	Block	1
79.183.26.212	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/109241.pdf	Block	1
66.249.64.240	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.116.228.134	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
185.27.105.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.67.48	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
81.218.74.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/sssssss=1eec5693sssssss_1eec5693	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
64.19.78.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.67.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1

11-20-2015-01:06:18 to 11-20-2015-02:06:18