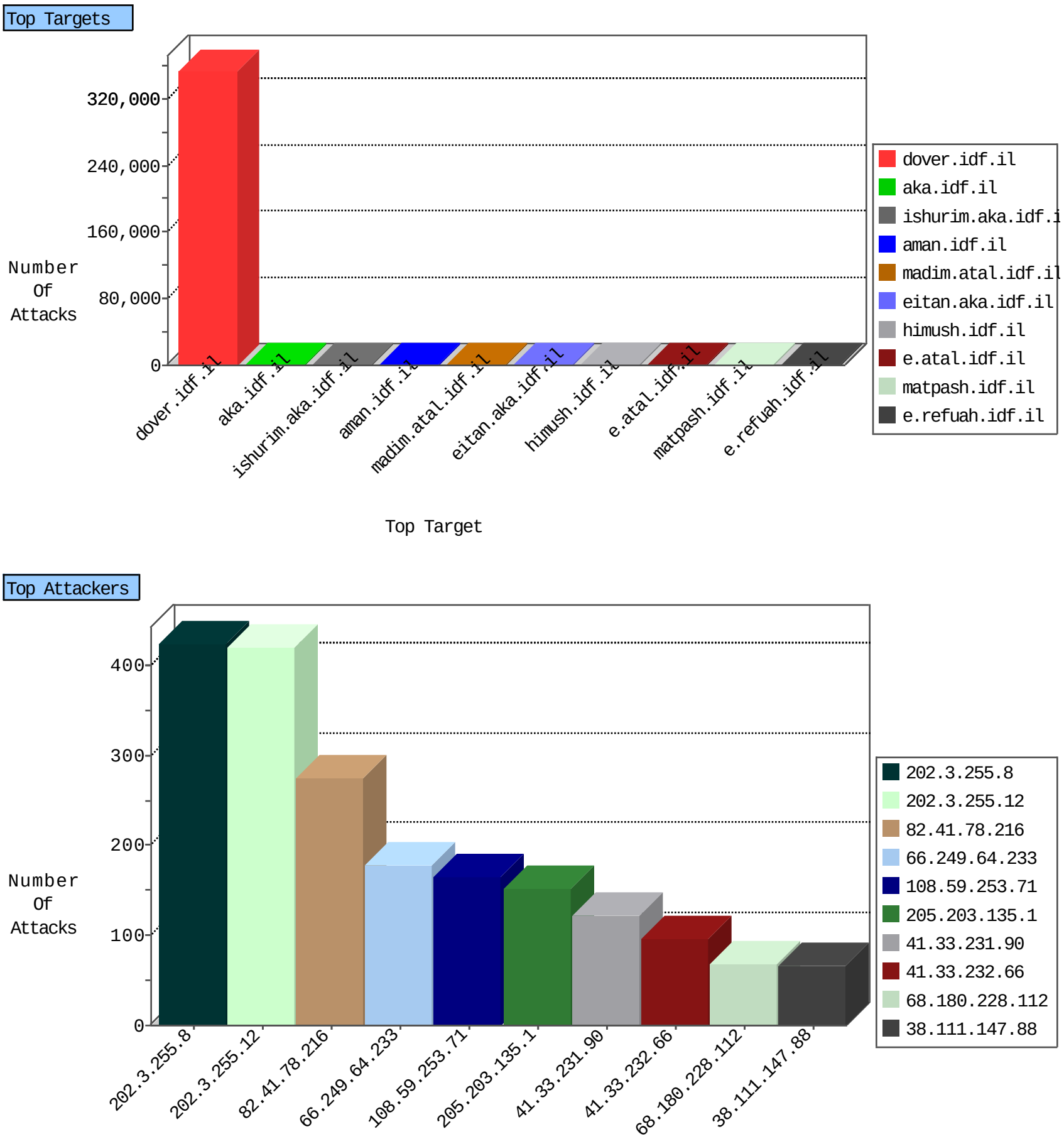
11-20-2015-03:04:03 to 11-20-2015-04:04:03

IDF Under Attack Daily Report



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3998
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
80.27.138.89	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
94.229.209.21	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
63.248.181.9	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
195.209.101.111	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
216.114.50.36	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
81.170.141.53	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
177.87.186.120	Brazil	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
63.248.130.8	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
98.167.196.47	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.180.104	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.151.233.124	Slovenia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.92.213.89	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.241.154.10	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
70.73.75.43	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
169.236.135.28	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.131.176.15	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.88.107.6	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
202.21.136.9	New Zealand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.199.42	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
87.227.145.34	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.142.40.26	Finland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.0.24.96	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.68.238.5	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
109.125.212.78	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.58.64.81	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.150.114	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
187.16.91.31	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.86.58.59	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.93.63.111	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.220.180.124	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
95.155.66.110	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.155.6	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
45.74.174.57		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.193.106	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.118.168.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.241.154.10	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
69.114.177.24	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
154.20.176.11	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.226.225.125	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.233.198.2	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.84.245.41	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
191.121.165.84	Brazil	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
66.185.213.99	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.177	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	388
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	384
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	3
150.126.50.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.173.61	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.49.71	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.102.214.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.117.209.135	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
170.106.47.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.112.104	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.106.222.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.60.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.155.92	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.65.81	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.27.247.115	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.207.9	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.224.28.26	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.50.22	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.138.9	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.57.64	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.30.96	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.75.100	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.242.3	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.34.59	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.189.113	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.59.35	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.198.163.75	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.45.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.204.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
178.159.191.31	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.200.40	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.16.101	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.153.120	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.73.228.130	147.237.76.201	Singapore	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
199.34.186.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.190.39	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.59.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.0.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.194.77	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.71.20	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.105.68.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.113	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
199.26.118.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.119.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.56.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.73.228.130	147.237.76.201	Singapore	e.atal.idf.il	ET SCAN NMAP -f -sS	1
130.201.176.28	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
208.90.2.110	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.41.78.216	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	275
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	166
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	116
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
200.49.206.196	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
200.49.193.195	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
200.49.193.194	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
200.49.206.194	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
200.49.206.195	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
108.72.12.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
185.3.146.254	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
200.49.206.193	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
184.173.238.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
77.125.113.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
178.63.55.202	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
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
65.19.138.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
85.214.11.209	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
185.3.146.254	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	15
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.63.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.61.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
173.75.224.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.251.191.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.103.152	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.117.189.195	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
87.117.189.195	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.117.189.195	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
46.19.85.233	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
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.230	Block	1
141.212.122.112	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	1
79.176.149.33	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
40.77.167.11	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kapatz/	Block	1
115.31.175.92	Thailand	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
171.124.56.221	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
115.31.175.92	Thailand	147.237.72.156	aman.idf.il	eMail Hoarding	Block	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
115.230.126.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/resources/styles/pratim.css	Block	1
204.93.154.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
87.117.189.195	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
62.25.16.234	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/localauth/setaccount.aspx	Block	1
131.162.130.180	Canada	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.67.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

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