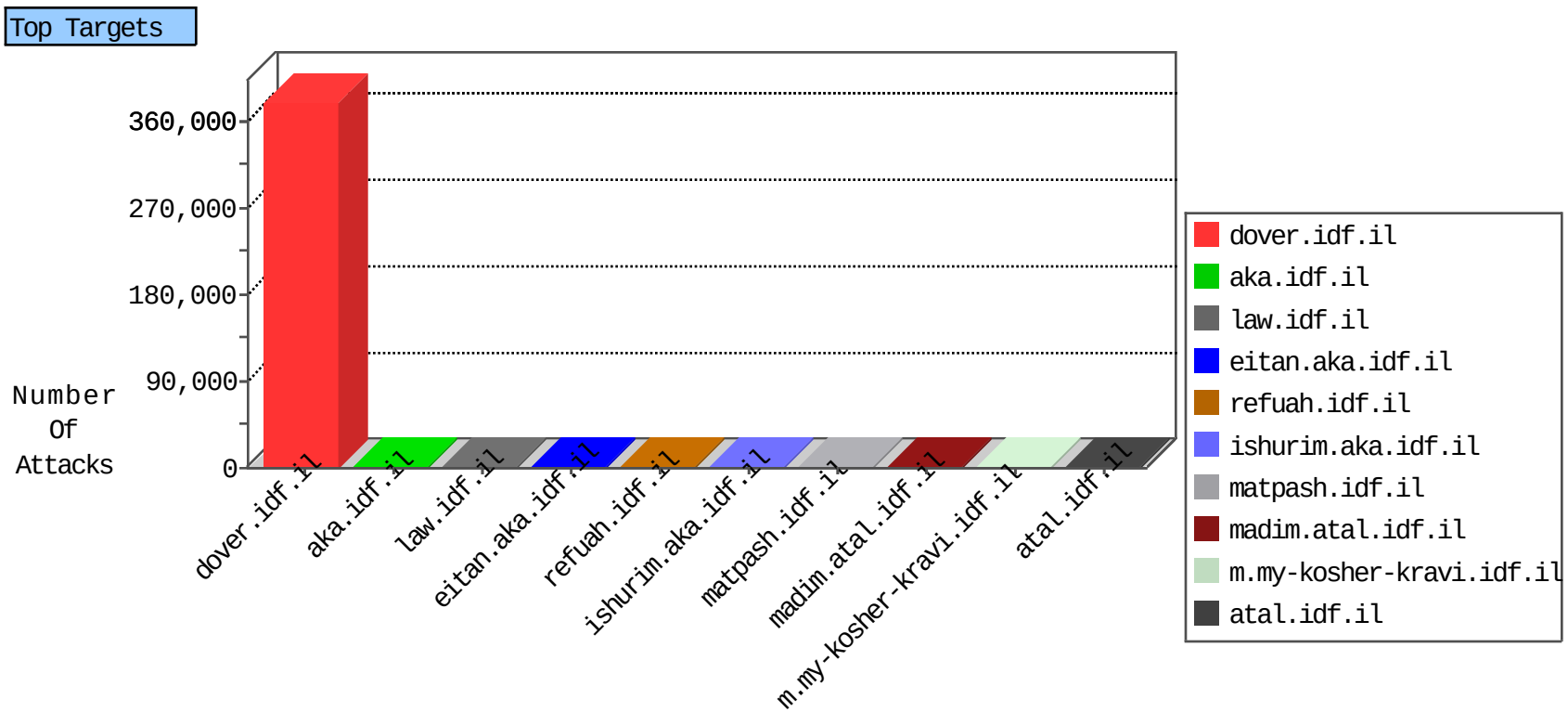
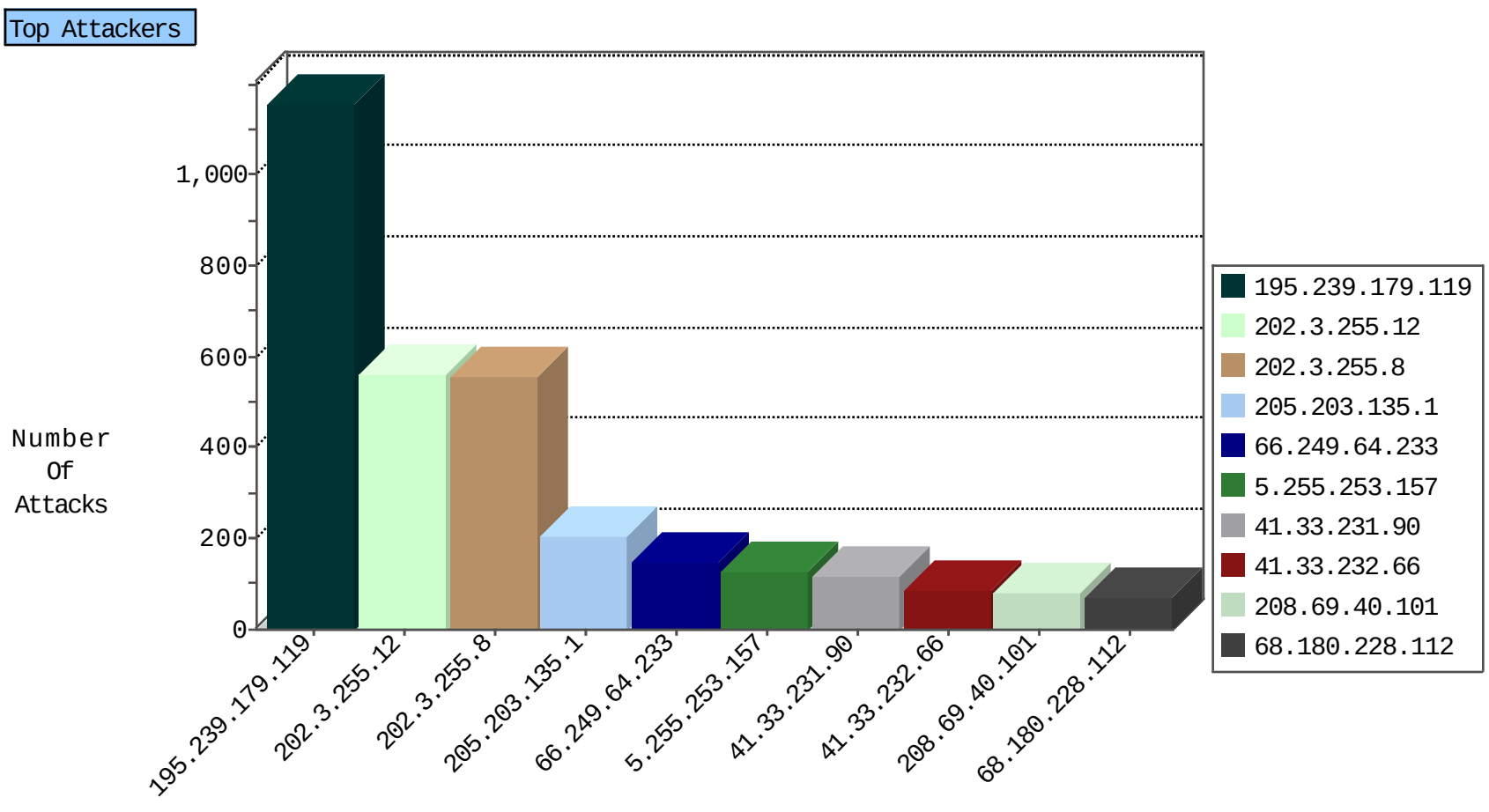
11-20-2015-04:04:06 to 11-20-2015-05:04:06

IDF Under Attack Daily Report



Top Target



Top Attackers

11-20-2015-04:04:06 to 11-20-2015-05:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.216	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	7
209.40.138.40	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
95.173.45.82	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
24.51.116.124	Bahamas	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
71.14.172.32	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
94.135.218.105	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
128.127.85.7	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
64.92.147.127	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
89.65.1.1	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
68.14.128.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
46.59.75.116	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.68.56	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
201.32.147.106	Brazil	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
69.84.242.27	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
108.59.65.85	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.241.90.100	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
96.48.150.27	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
218.144.200.49	Korea, Republic of	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
31.208.92.31	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.142.3.84	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.187.65	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.148.117.86	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.111.48.64	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.214.128.3	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.198.21	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.197.133.2	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.170.120	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
87.104.132.2	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.33.242.98	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
71.195.91.57	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.4.193.203	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
69.200.247.102	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
110.21.162.21	Australia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.221.232.47	China	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
84.232.99.60	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.219.205.69	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
199.61.180.29	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
68.241.42.84	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
99.245.53.33	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
37.200.44.72	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
95.34.212.71	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.196.154.54	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.11.251.11	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
81.246.137.42	Belgium	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.132.102	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
173.52.158.115	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.233.66	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-20-2015-04:04:06 to 11-20-2015-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-20-2015-04:04:06 to 11-20-2015-05:04:06

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	526
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	518
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
170.113.74.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.69.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.83.84	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.14.1.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.149.29	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.39.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.155.23	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.174.4.116	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.101.243.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.50.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.21.9	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.197.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.172.56	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.178.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.190.56	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.83.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.204.17	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
74.117.209.136	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.255.57	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.150.95	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
129.76.99.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.224.166.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.153.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.122.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.138.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.107.60	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.230.85.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.223.40	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.132.46	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
170.67.157.93	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.136.77	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.209.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.228.121	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.203.239.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.243.55	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.92.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.211.216.28	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.249.41	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.205.93.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.111.102	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.58.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
170.67.98.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.97.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-20-2015-04:04:06 to 11-20-2015-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.239.179.119	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1144
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	204
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	128
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	85
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	85
208.69.40.101	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	80
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
179.148.253.192	Brazil	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	69
72.89.152.221	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
76.222.215.72	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
50.87.144.145	United States	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	38
209.6.148.106	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	24
158.69.2.151	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
98.203.59.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
204.93.154.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
186.176.24.178	Costa Rica	147.237.77.216	dover.idf.i	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
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
88.198.25.217	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
65.19.138.33	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
204.12.168.26	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
67.85.176.123	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
66.249.64.243	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
107.170.62.43	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
104.131.197.228	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
181.197.160.142	Panama	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
176.12.139.178	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
172.56.5.184	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
37.26.146.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.203.103.152	Greece	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
98.169.20.31	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10

11-20-2015-04:04:06 to 11-20-2015-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.63.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	4
82.81.10.196	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.19.85.233	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
66.249.67.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
204.12.168.26	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.12.168.26	United States	147.237.72.166	aka.idf.il	Multiple signatures from 204.12.168.26	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.64.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3132.doc	Block	1
141.212.122.112	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1
66.249.67.41	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3131.pdf	Block	1
174.57.78.19	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.67.46	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18063-he/dover.aspx	Block	1
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1

11-20-2015-04:04:06 to 11-20-2015-05:04:06