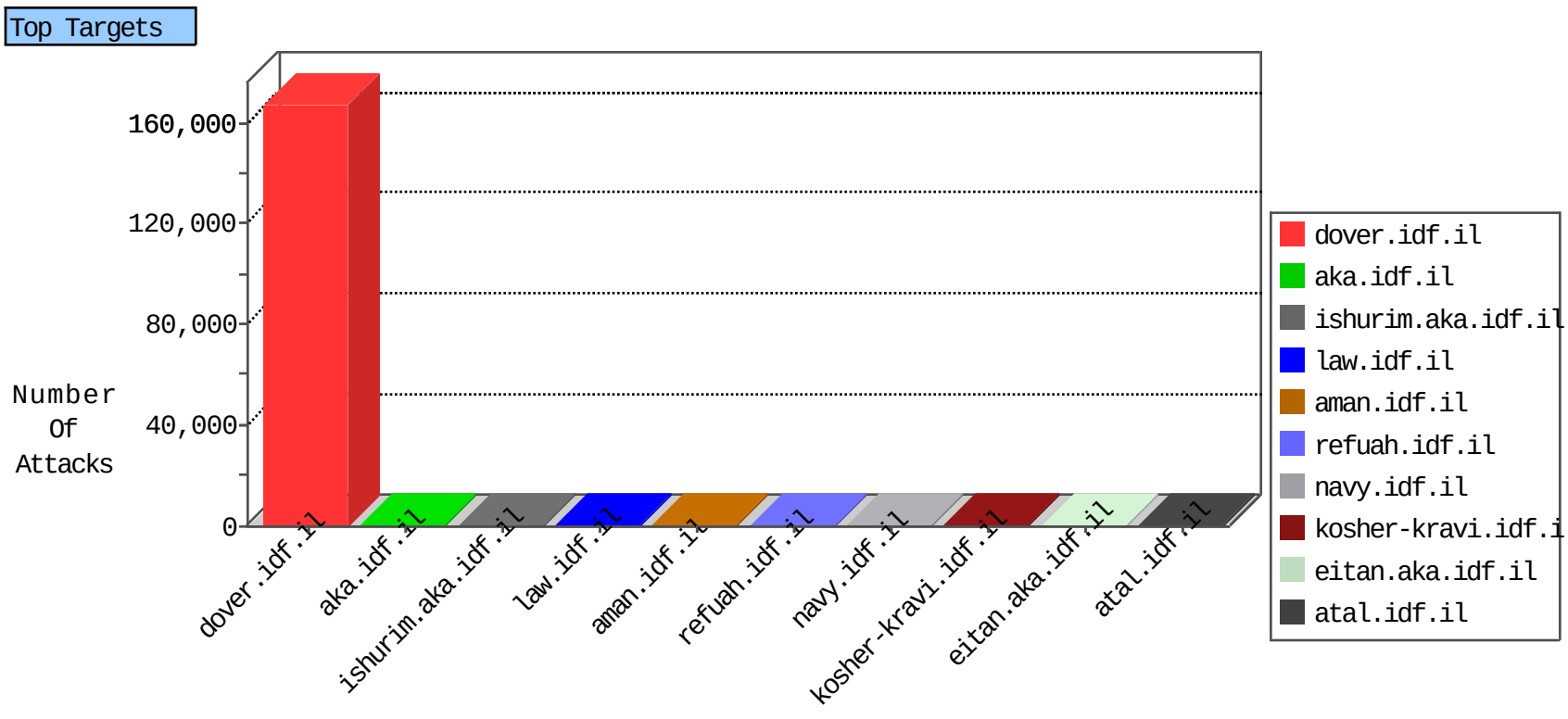
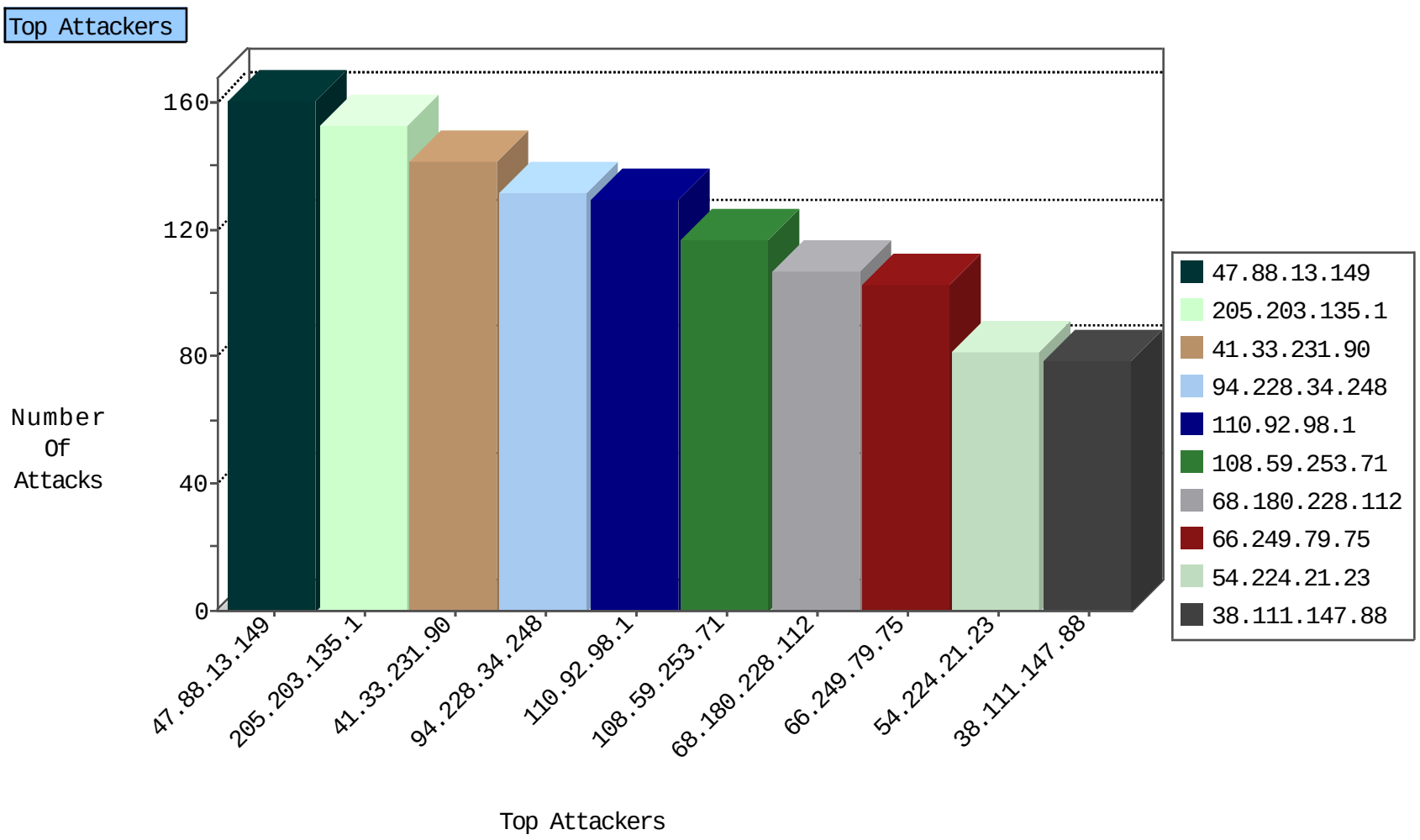
11-16-2015-03:04:01 to 11-16-2015-04:04:01

IDF Under Attack Daily Report





11-16-2015-03:04:01 to 11-16-2015-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.127	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7222
66.249.78.254	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3272
126.207.166.114	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3201
120.172.90.44	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3188
190.231.164.83	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3024
123.108.236.127	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2982
207.238.77.37	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2958
140.219.68.32	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2944
160.198.13.57	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2935
1.160.109.47	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2564
60.187.87.94	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	525
222.219.62.64	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	427
126.79.20.21	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	363
220.181.108.143	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	360
222.78.200.82	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	310
179.93.199.123	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	266
177.121.234.83	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	257
120.185.136.53	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	248
220.143.1.25	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	173
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	169
175.205.120.101	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	159
181.69.173.28	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	152
186.123.168.6	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	145
120.185.188.123	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	134
115.54.19.45	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	126
207.80.52.19	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
195.170.185.25	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	95
89.253.102.35	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	88
182.231.169.2	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	78
59.28.255.52	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
122.116.135.115	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
133.64.249.99	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	38
207.126.54.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36
177.109.31.11	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
130.113.112.124	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
171.111.239.86	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
216.158.212.25	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
99.252.147.87	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
66.185.202.108	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
50.190.1.127	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
162.220.204.92	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
72.42.90.74	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
89.160.39.32	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
76.76.85.127	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
119.57.65.89	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
193.91.245.123	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.49.210.85	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.152.23	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
162.252.112.59	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.209.48.74	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-16-2015-03:04:01 to 11-16-2015-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.201	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.138	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-16-2015-03:04:01 to 11-16-2015-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
138.43.48.71	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.72.34	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
81.31.244.14	147.237.0.15	Iran, Islamic Republic of	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
143.135.88.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.127.70	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.10.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.110.183.58	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.214.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.106.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.159.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.105.121.44	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.202.100.17	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.189.67	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.211.216.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.95.203.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.200.64	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.86.98	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
121.46.76.47	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.20.95	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.4.22	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.132.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.22.214.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.201.36	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
180.153.104.125	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
119.90.138.60	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
140.170.58.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.99.87	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.209.85.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.77.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.174.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.224.61	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.252.13	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.8.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.187.234.119	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
129.76.110.56	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.193.61	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.64	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
95.216.29.60	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.227.76	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.44.37	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.196.218.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.147.121	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.48.9	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.42.131.106	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.22.30	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.184.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.60.119	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.127.104	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-16-2015-03:04:01 to 11-16-2015-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
47.88.13.149	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	161
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
54.226.126.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
166.137.252.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
213.57.72.76	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
95.23.232.83	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
87.69.34.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.79.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	44
104.158.24.21	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.79.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
70.138.169.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
79.176.159.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.79.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
109.65.10.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
216.4.56.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.65.10.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
157.55.39.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
157.55.39.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.24.181.135	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
80.178.187.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
162.104.238.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
188.165.15.233	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
187.20.116.117	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
157.55.39.139	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
157.55.39.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.62.43	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
104.131.195.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.131.200.249	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	12

11-16-2015-03:04:01 to 11-16-2015-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
67.82.74.161	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
40.117.44.123	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
84.108.1.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″×ª× ×“×‘×ª	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2799.jpg	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1243-he/atal.aspx	Block	1
111.170.68.200	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/newsflash/www.ynet.co.il	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1239-he/atal.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/62953.jpg	Block	1
66.249.67.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2330.jpg	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.67.237	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1

11-16-2015-03:04:01 to 11-16-2015-04:04:01