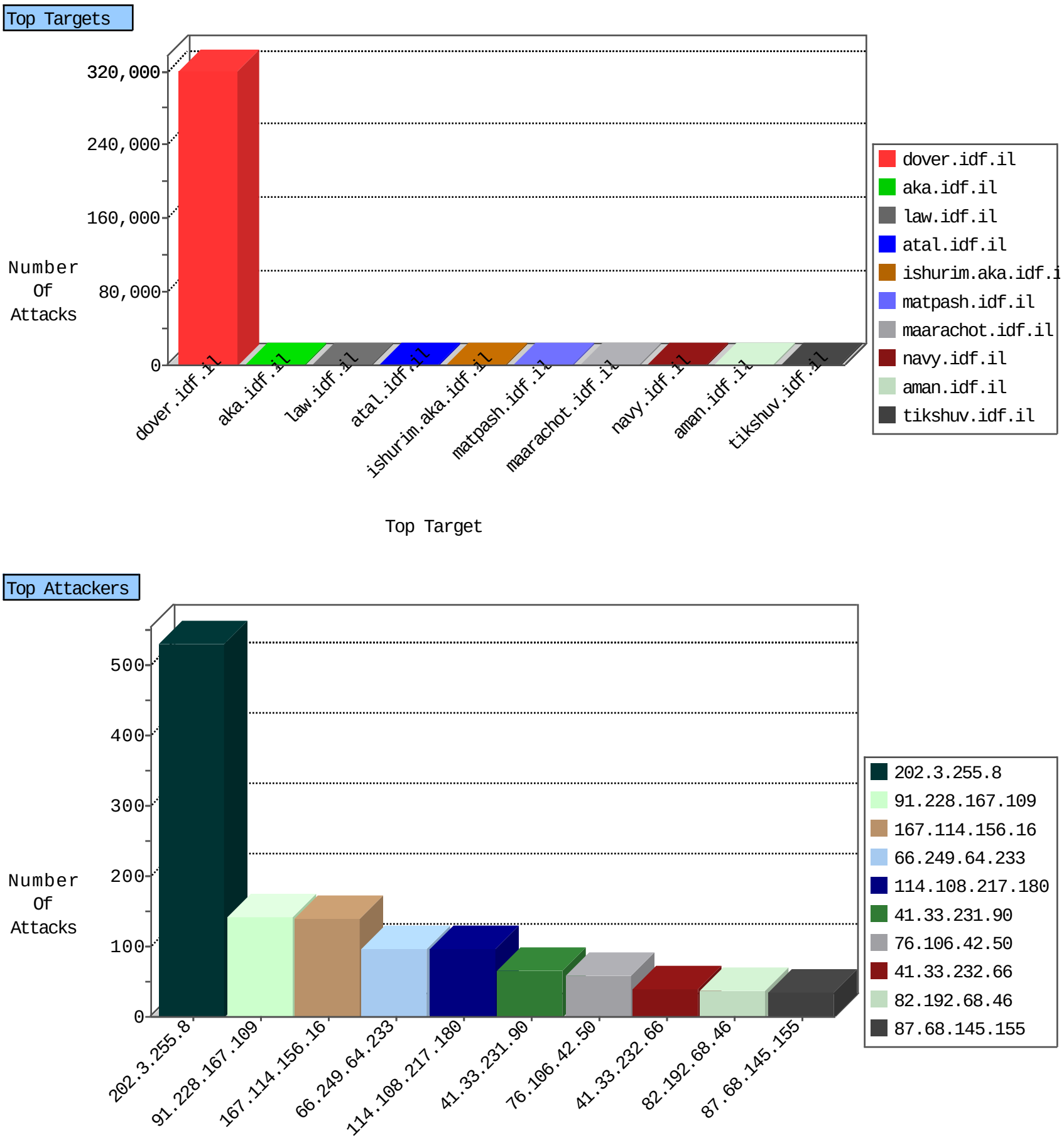
11-18-2015-04:04:01 to 11-18-2015-05:04:01

IDF Under Attack Daily Report



11-18-2015-04:04:01 to 11-18-2015-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6050
73.189.144.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3940
123.247.222.4	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2931
86.127.165.54	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2901
114.238.153.121	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2756
216.244.222.1	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2516
66.249.78.242	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	630
190.213.31.28	Trinidad and Tobago	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	197
97.77.59.9	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	197
118.57.226.124	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	194
175.207.144.124	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	189
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	177
201.83.153.93	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	168
45.49.94.121		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	149
151.245.19.51	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	142
129.12.25.52	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	106
64.184.115.110	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	82
123.8.237.11	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	69
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
128.189.182.120	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
94.143.1.18	Switzerland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
46.59.27.123	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.18.177.76	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
63.248.101.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
5.150.242.60	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
201.220.157.118	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
82.68.47.55	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
219.97.185.90	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
89.21.216.84	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
135.23.218.109	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
64.92.137.109	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
74.14.196.74	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
63.248.131.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.89.88.114	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
122.154.33.88	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.93.251.127	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.208.4.74	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.209.227.74	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.191.41	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
180.214.56.0	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.63.50.18	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.70.152.37	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.138.210.114	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.55.27	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.127.59	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.48.207.122	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.212.195.98	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-18-2015-04:04:01 to 11-18-2015-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.27.98.173	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

11-18-2015-04:04:01 to 11-18-2015-05:04:01

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	496
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
198.48.17.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.161.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.189.25	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.32.139.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.132.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.82.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
203.197.205.118	147.237.76.148	India	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
157.232.0.76	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.141.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.117.50	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.136.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.225.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.93.80	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.22.223.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.198.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.30.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.215.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.125.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
216.212.206.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.50.63	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.220.119	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.211.218.66	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.175.53	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.224.170.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.172.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.225.73	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.105.121.63	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.151.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.114.71	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.57.72	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.109.99.21	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.5.64	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.83.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.179.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.230.91.6	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.103.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.48.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.134.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.78.35	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.117.12	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.217.67	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.88.52	147.237.76.38	Singapore	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.148.67.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.247.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.248.109	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.29.46	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-18-2015-04:04:01 to 11-18-2015-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
114.108.217.180	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
76.106.42.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.64.149	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
50.127.29.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
87.68.145.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
177.237.49.41	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
71.13.10.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
73.189.144.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
82.80.27.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
87.68.145.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.52.141.109	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
186.31.220.19	Colombia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.34.224.235	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
71.190.233.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
178.22.66.120	Switzerland	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
184.172.196.102	United States	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
107.170.62.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
99.226.110.175	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.115.154.109	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
24.113.221.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.28.180.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

11-18-2015-04:04:01 to 11-18-2015-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.27.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.201.224.8	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
109.186.52.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.40.129.123	Block	1
112.201.245.96	Philippines	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.120.165.144	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
112.201.245.96	Philippines	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69861.jpg	Block	1
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
141.212.121.192	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	1
74.82.47.3	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
100.37.117.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	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
74.82.47.4	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 193.201.224.8	Block	1

11-18-2015-04:04:01 to 11-18-2015-05:04:01