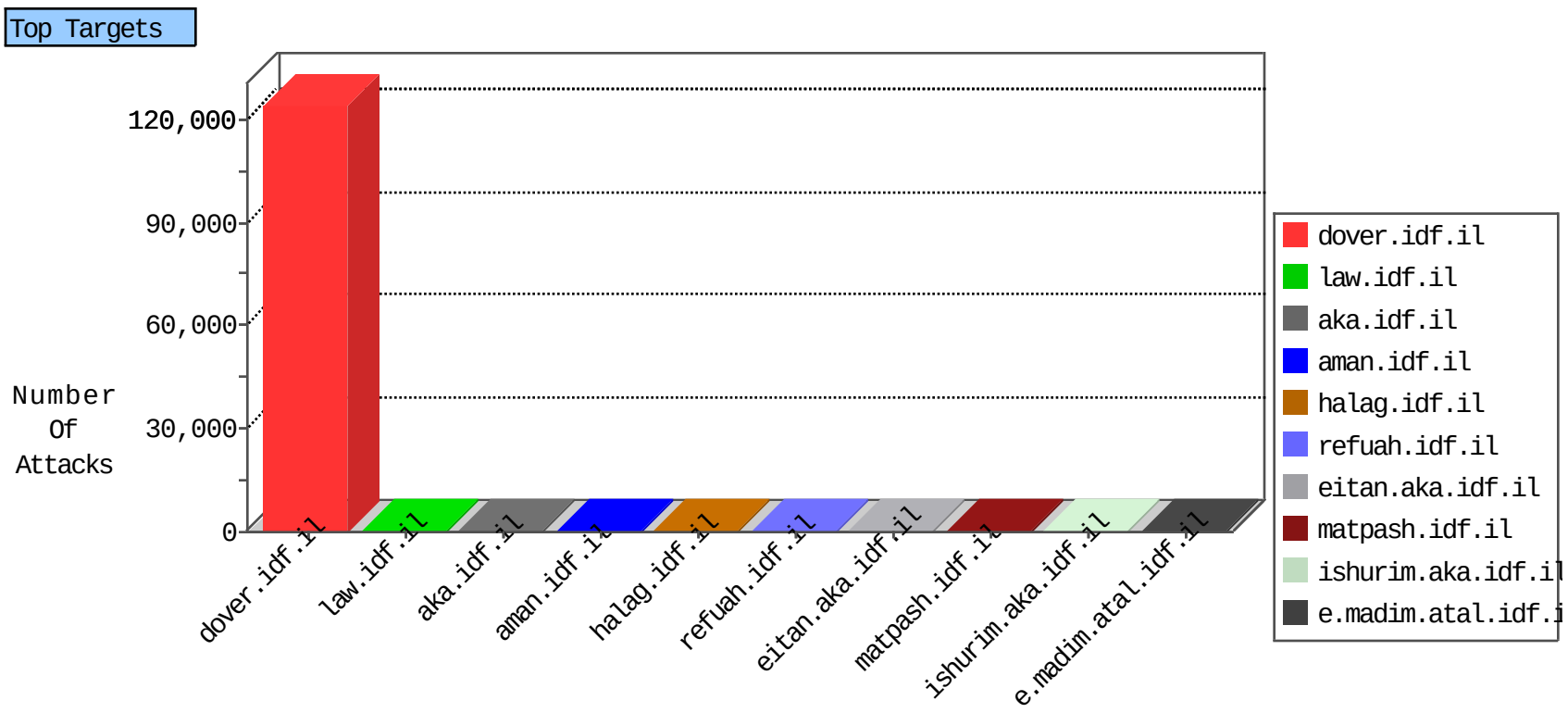
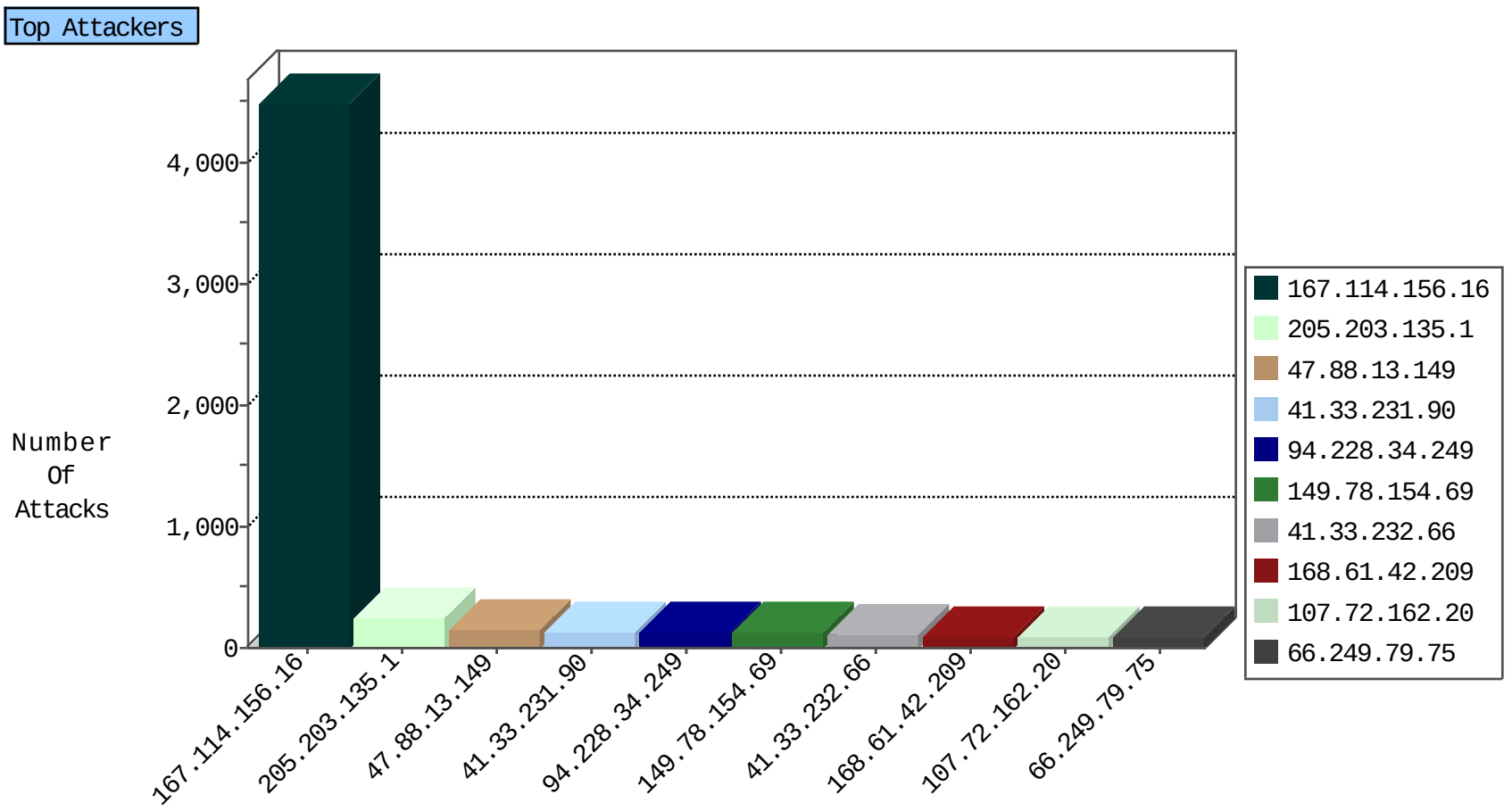
11-16-2015-04:04:04 to 11-16-2015-05:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-16-2015-04:04:04 to 11-16-2015-05:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.53.25.99	Thailand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3354
191.27.176.13	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3232
121.42.13.59	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3003
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	209
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	172
122.102.185.87	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	127
104.79.3.48	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	116
117.80.154.10	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42
222.115.162.80	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
111.39.250.115	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28
210.4.60.30	Philippines	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
128.107.214.84	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
124.254.203.67	Korea, Republic of	147.237.76.201	e.atal.idf.i	Block_Udp_All_Nets	drop	4
94.135.209.43	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
74.81.238.41	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
24.105.234.122	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
83.233.133.26	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
84.211.146.3	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
74.81.237.93	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.139.41	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
108.162.162.80	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.255.180.70	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.172.91	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
61.80.17.17	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
189.206.102.17	Mexico	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
12.238.188.31	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.159.142.68	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.76.80.71	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.48.242.110	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
73.17.118.15	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.137.249.60	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
110.20.27.123	Australia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
100.42.161.103	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.103.65	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
37.19.41.19	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
186.104.76.49	Chile	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.88.100.26	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
218.25.78.59	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
144.216.114.17	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.209.182.93	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.178.127	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
108.162.177.59	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.160.211.8	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.200.124.82	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.107.187.33	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.11.152.34	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.214.52	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.11.42.29	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
23.91.234.88	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
181.82.224.46	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-16-2015-04:04:04 to 11-16-2015-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.134.102.16	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	3
151.80.31.131	Italy	147.237.76.31	nakchal.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
151.80.31.133	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.64	France	147.237.76.147	chinuch.aka.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

11-16-2015-04:04:04 to 11-16-2015-05:04:04

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
119.38.224.98	147.237.77.216	China	dover.idf.il	GPL SCAN nmap TCP	4
203.86.7.130	147.237.77.216	China	dover.idf.il	GPL SCAN nmap TCP	4
66.249.79.6	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
159.226.33.6	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
130.201.187.92	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.212.109.34	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.132.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.110.58.26	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.73.89	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.53.103	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.189.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.102.186.35	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
209.205.216.95	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.34.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.226.33.6	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
130.201.111.56	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.165.47.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.6.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.35.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.132.127	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.189.13.36	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.250.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.51.26	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.24.16	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.183.38.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.185.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.143.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.226.33.6	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
167.97.200.6	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.206.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.203.225.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.188.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.141.59	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.162.210.3	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.199.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.219.32	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.176.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.4.102	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.50.114	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.175.170.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.1.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.187.125	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.103.89	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.16.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.15.3.93	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.78.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.229.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-16-2015-04:04:04 to 11-16-2015-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4388
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	255
47.88.13.149	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	155
94.228.34.249	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	133
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	123
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	114
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	98
107.72.162.20	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	97
168.61.42.209	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	97
54.226.126.170	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	73
66.249.79.75	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
159.53.78.140	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
65.129.167.2	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
195.239.179.119	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	43
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
109.65.10.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
52.33.66.29	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
109.65.10.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
52.28.181.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
104.131.197.228	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
128.4.218.153	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
66.249.79.79	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
66.249.69.128	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
128.242.249.11	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
88.198.157.214	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
66.249.79.75	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
66.249.79.77	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
204.93.154.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
87.68.145.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
87.68.145.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
107.72.162.33	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
107.170.63.50	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
104.131.195.214	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
188.165.15.233	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
65.19.138.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
157.55.39.248	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12

11-16-2015-04:04:04 to 11-16-2015-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/pdficon.gif	Block	1
66.249.65.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/108997.pdf	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
82.221.105.7	Iceland	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
40.77.167.30	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.8.142.29	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2800.jpg	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.31	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/fund/Ã£â€”Ã¢â‚¬Ëœ Ã£â€”Ã¢â‚¬Â?Ã£â€”Ã¢Â§Ã£â€”Ã¥Â¾Ã£â€”Ã¢â‚¬Â?	Block	1
180.76.15.163	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

11-16-2015-04:04:04 to 11-16-2015-05:04:04