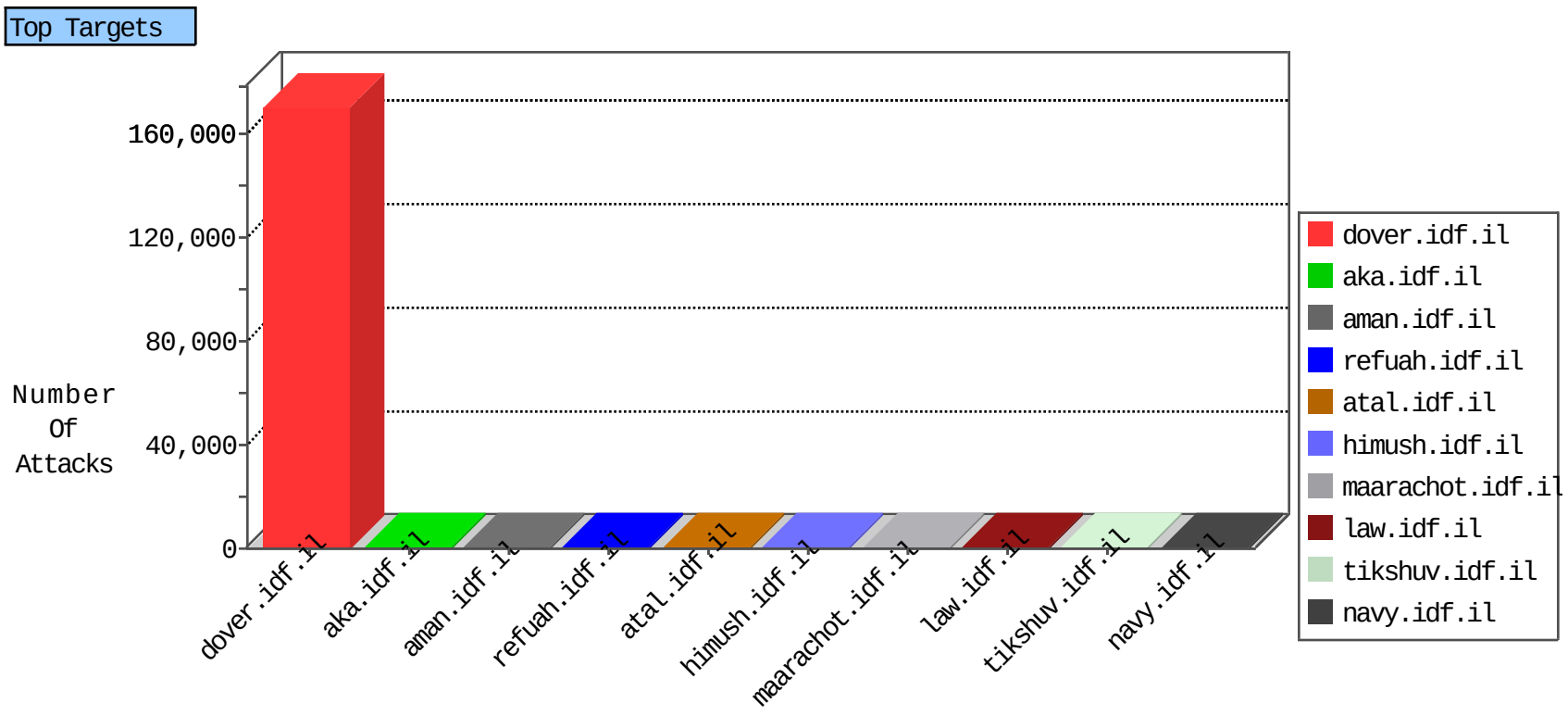
11-18-2015-01:06:50 to 11-18-2015-02:06:50

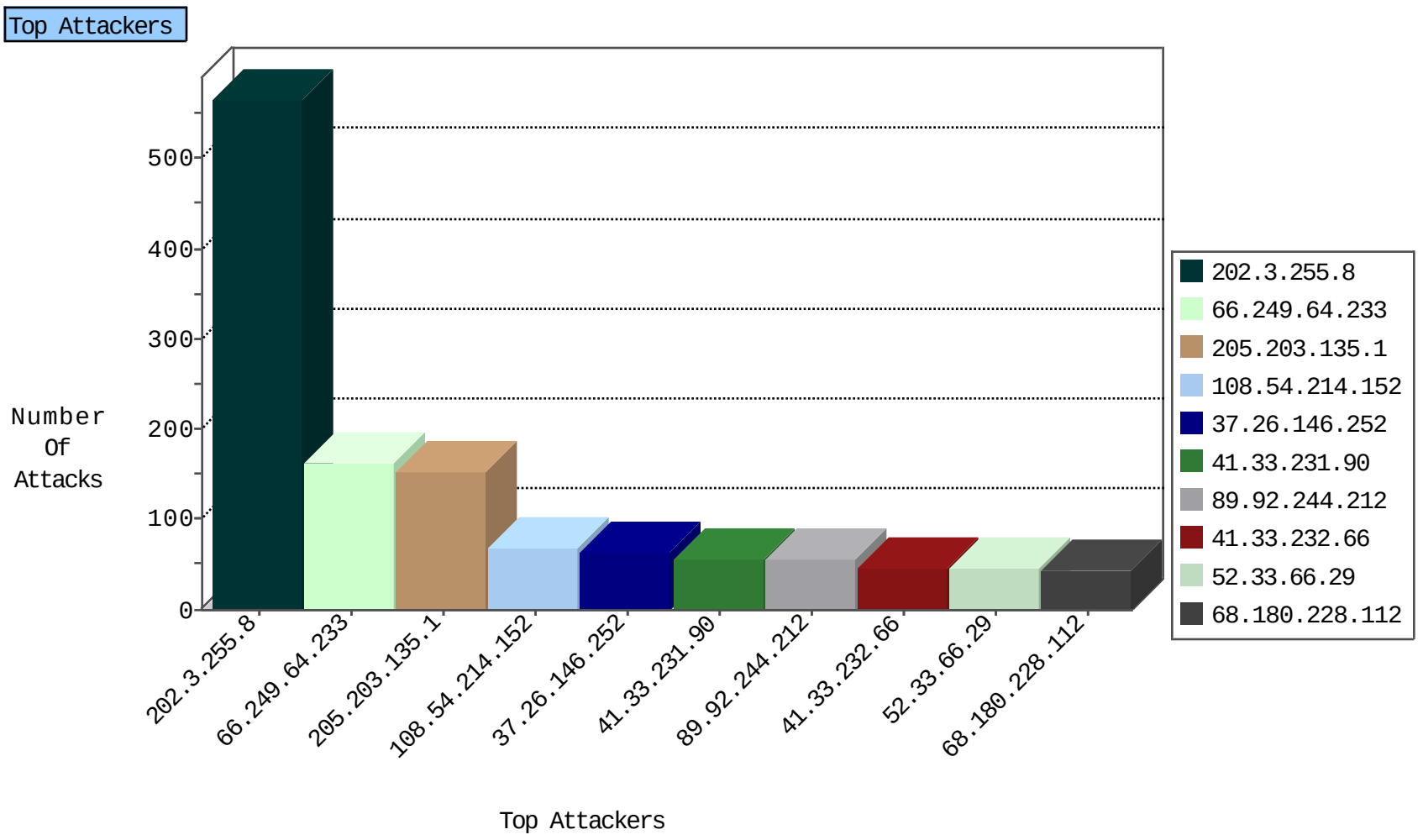
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-18-2015-01:06:50 to 11-18-2015-02:06:50

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.93	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2974
179.231.143.106	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2514
66.249.65.18	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2179
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1024
180.140.255.15	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	244
107.183.182.97	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	244
61.17.42.33	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	199
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	181
54.230.246.104	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	167
71.46.166.119	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	39
211.194.158.27	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
69.9.69.108	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
31.209.6.111	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
109.170.182.96	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
206.248.57.34	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
122.43.205.39	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
31.29.119.8	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
203.229.174.55	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
24.136.251.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.180.152.73	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.9.101	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.217.74	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.47.219.14	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.91.209.11	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
73.166.174.121	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
153.155.233.76	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
69.60.243.31	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.100.55.126	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
221.223.17.69	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.59.20.100	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.199.7.50	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
188.169.91.52	Georgia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
31.208.81.16	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.114.7	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
68.116.46.83	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
112.184.102.74	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.132.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.218.75.10	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
99.233.99.71	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
206.77.45.23	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.245.113.101	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
79.135.116.83	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.245.145.47	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
1.215.118.172	Korea, Republic of	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
76.76.66.50	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
162.255.33.84	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.69.230.74	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.254.12	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-18-2015-01:06:50 to 11-18-2015-02:06:50

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-18-2015-01:06:50 to 11-18-2015-02:06:50

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	528
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.109	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.176.116.200	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.101	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
184.154.42.62	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
88.135.18.93	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.186.35	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.107.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
50.204.188.142	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
207.32.155.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.94.221.68	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.22.1	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.22.117.95	147.237.77.216	Netherlands	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.189.66	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.102.186.35	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
206.203.94.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
98.119.105.221	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
157.231.42.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.10.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
134.172.111.47	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.236.1.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.245.24	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.225.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
134.172.63.20	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.151.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.47.21	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.65.109	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.15.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.86.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.244.23	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.19.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.230.73.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.205.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.245.13	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.64.230	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
143.49.164.101	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.34.177.109	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.191.13	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.4.105	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.77.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.174.171.104	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
138.43.158.20	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.156.45	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.22.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.174.171.104	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
128.168.216.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.27.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-18-2015-01:06:50 to 11-18-2015-02:06:50

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	153
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	146
108.54.214.152	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
37.26.146.252	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
89.92.244.212	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
52.33.66.29	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
63.249.66.212	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
92.8.225.137	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
192.0.101.58	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
41.239.175.102	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
98.220.37.173	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.64.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
192.0.100.35	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
82.165.137.121	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
40.77.167.53	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
156.34.216.212	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	13
100.127.128.144		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
107.170.63.50	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
107.178.194.87	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
37.26.148.237	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
176.12.145.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
46.166.186.197	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
193.171.202.150	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
40.143.1.4	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
87.203.103.152	Greece	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
107.178.194.79	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
109.190.166.99	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
176.12.145.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
1.129.96.68	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
37.142.64.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.110.29.18	Latvia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
66.249.64.233	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
31.168.187.169	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
192.0.100.203	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
192.0.101.35	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
207.210.130.125	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8

11-18-2015-01:06:50 to 11-18-2015-02:06:50

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	4
109.66.179.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	2
116.87.74.77	Singapore	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
185.49.14.190	Poland	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
89.247.8.35	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
185.25.148.240	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.73.181	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	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/6/size100x0/3156.jpg	Block	1
185.25.148.240	Poland	147.237.76.30	himush.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.65.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
66.249.73.189	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/940.pdf	Block	1
66.249.64.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3369.jpg	Block	1
185.25.148.240	Poland	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
81.218.154.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
5.29.245.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.150.214.90	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.67.1.208	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.75.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18489-he/dover.aspx	Block	1
185.25.151.159	Poland	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
85.219.143.163	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.123.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

11-18-2015-01:06:50 to 11-18-2015-02:06:50