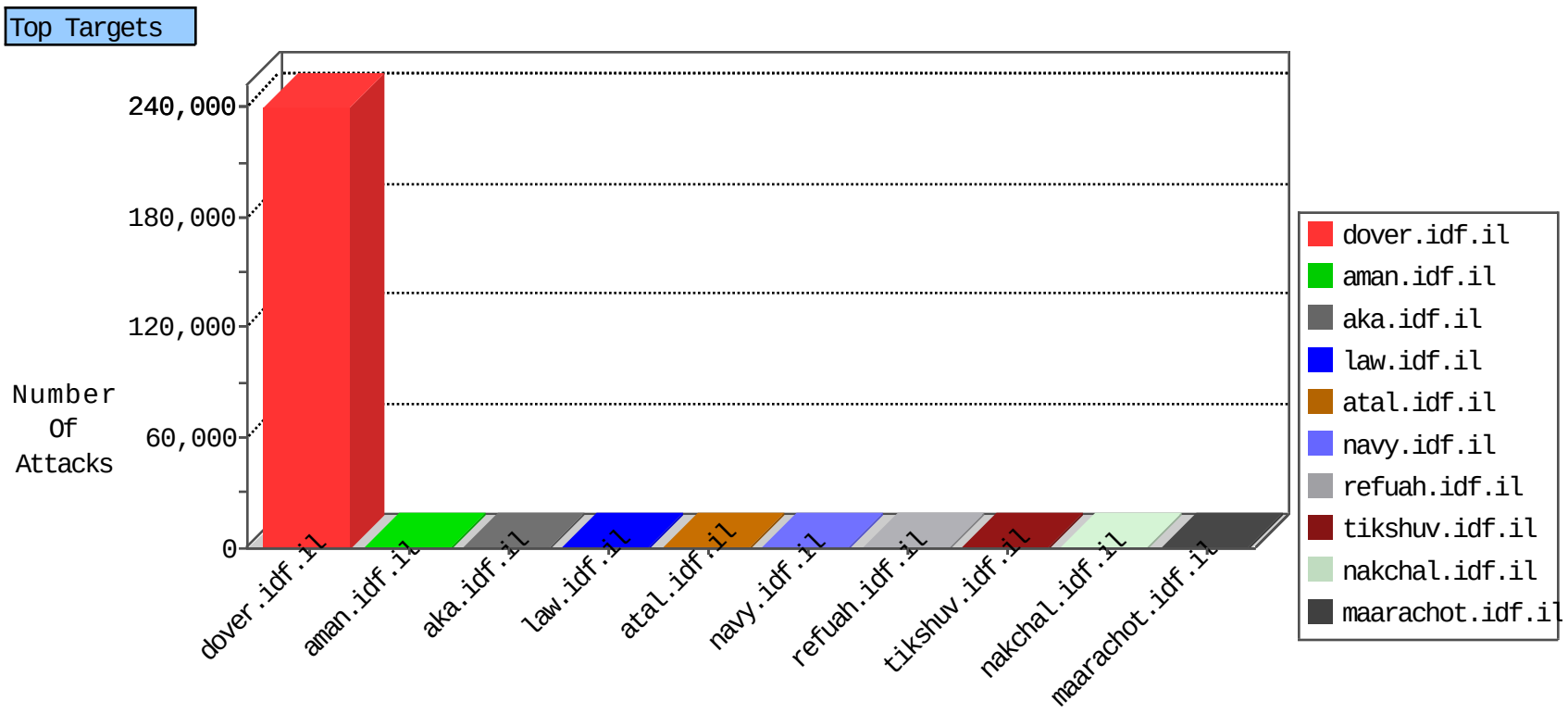
11-18-2015-03:04:05 to 11-18-2015-04:04:05

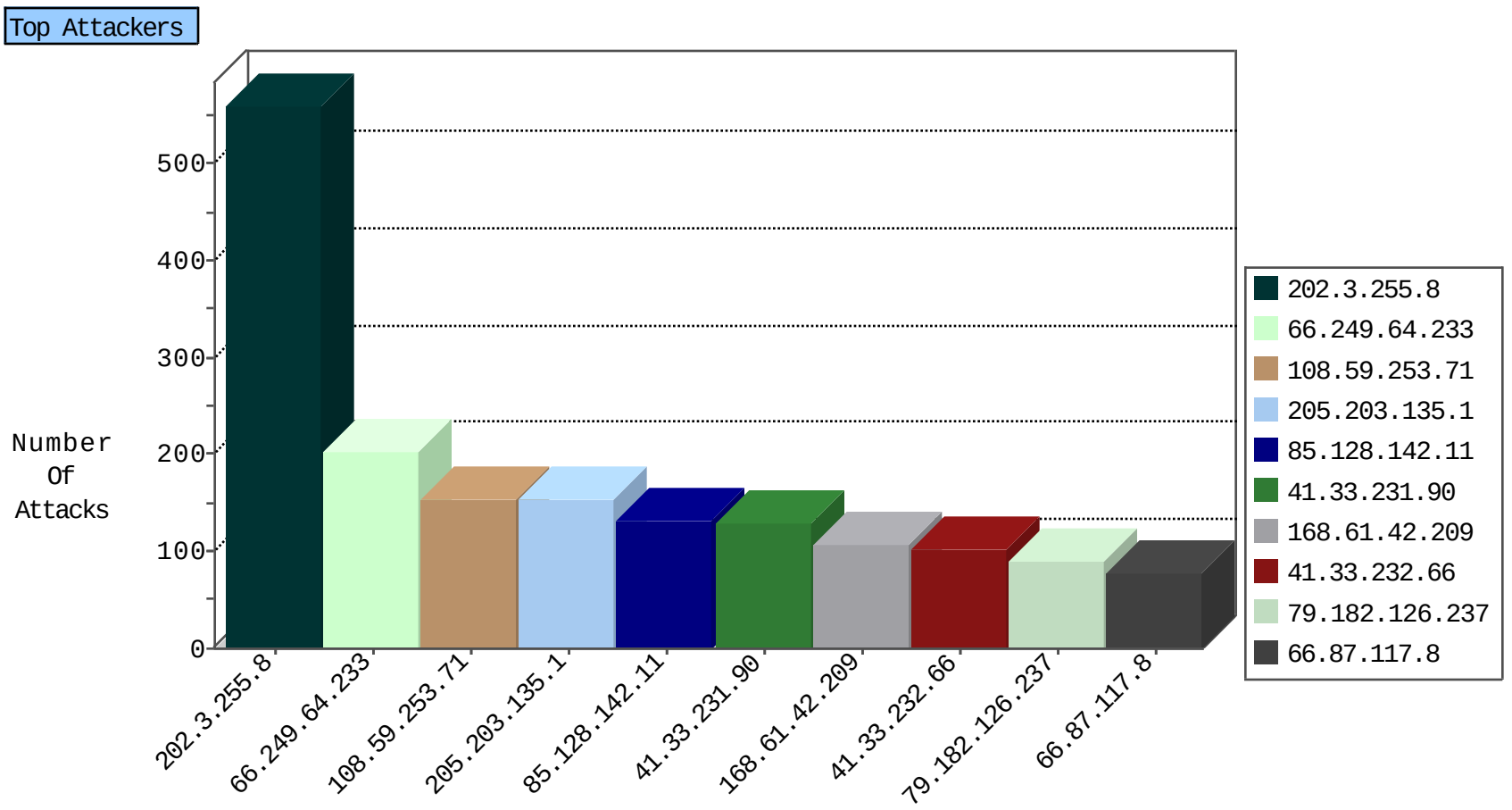
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-18-2015-03:04:05 to 11-18-2015-04:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.37	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4521
125.118.44.119	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3041
116.235.2.84	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3006
122.178.169.98	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2967
194.83.240.46	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2874
177.9.225.6	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2700
200.72.3.112	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2653
71.47.247.10	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2620
165.199.183.0	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2609
54.204.252.202	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	729
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	665
122.234.192.119	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	499
108.54.106.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	435
126.61.213.59	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	421
58.19.160.105	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	386
126.217.155.101	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	233
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	175
180.71.223.121	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	148
118.92.159.68	New Zealand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	144
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	128
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	101
14.82.203.19	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	93
13.30.147.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	74
190.85.34.26	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	74
201.223.148.39	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	56
179.250.35.91	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	39
66.255.230.54	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
54.94.69.93	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
85.250.56.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
78.28.219.98	Latvia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
67.102.30.31	United States	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
178.248.100.3	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
58.177.46.67	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
24.70.10.0	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.112.94	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.225.191.97	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
110.159.152.14	Malaysia	147.237.77.216	dover.idf.il	Invalid L4 Header Length	drop	1
63.248.234.45	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
105.235.108.121	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.182.248.31	Austria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.99.23.17	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
175.125.177.66	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
77.57.91.91	Switzerland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.80.170.69	Ukraine	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.161.12	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
50.16.33.115	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.233.214.83	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-18-2015-03:04:05 to 11-18-2015-04:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.233.102.105	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5

11-18-2015-03:04:05 to 11-18-2015-04:04:05

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	522
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
194.24.179.104	147.237.76.30	Romania	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.37	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
194.24.179.104	147.237.76.176	Romania	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.93	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
194.24.179.104	147.237.77.74	Romania	law.idf.il	ET SCAN Potential SSH Scan	2
170.113.6.61	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.72.217	United States	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
207.22.254.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.35.95	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.176.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.42.135.46	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
194.24.179.104	147.237.77.19	Romania	law-forum.idf.il	ET SCAN Potential SSH Scan	1
121.46.115.86	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.224.28.109	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
204.106.215.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.132.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
194.24.179.104	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
110.44.131.38	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.253.80	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.40.100	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
204.93.154.201	147.237.77.216	United States	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
134.209.167.7	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
194.24.179.104	147.237.76.147	Romania	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
95.217.34.91	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.59.26	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.71.0.111	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.152.54	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.74.76	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.148.110	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.234.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.198.185.26	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.116.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.26.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.211.222.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.92.16	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.109.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.107.16.206	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.88.52	147.237.76.201	Singapore	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
157.231.89.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.212.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.16.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.219.197.115	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.29.68	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.88.52	147.237.76.200	Singapore	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-18-2015-03:04:05 to 11-18-2015-04:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	156
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	154
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	153
85.128.142.11	Poland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	131
168.61.42.209	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	108
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	98
66.87.117.8	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	78
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	76
37.26.148.218	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	73
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
188.247.81.158	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
5.175.0.137	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
83.169.10.185	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
79.182.126.237	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
79.182.126.237	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	43
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
100.37.214.241	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
17.142.156.109	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
173.208.186.42	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
128.242.249.12	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
54.204.252.202	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	22
54.158.169.77	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
100.127.128.144		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
50.16.33.115	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
210.87.255.225	Hong Kong	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
37.201.169.164	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
204.93.154.201	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
162.243.69.172	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
99.225.67.165	Canada	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
66.249.64.230	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
46.19.85.212	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
109.201.152.251	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11

11-18-2015-03:04:05 to 11-18-2015-04:04:05

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	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
5.29.245.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.138.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.18	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
191.102.204.8	Colombia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
47.21.57.190	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
80.246.130.60	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
204.93.154.201	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
128.232.110.28	United Kingdom	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
8.37.71.56	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/894-he/himush.aspx&usg=alkjrhj6jmtw0ah0uekosp3bucqci2rl1a	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19798-he/idfgdover.aspx	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
185.49.14.190	Poland	147.237.77.233	atal.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
46.116.132.175	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/journalview/journalview.aspx	Block	1

11-18-2015-03:04:05 to 11-18-2015-04:04:05