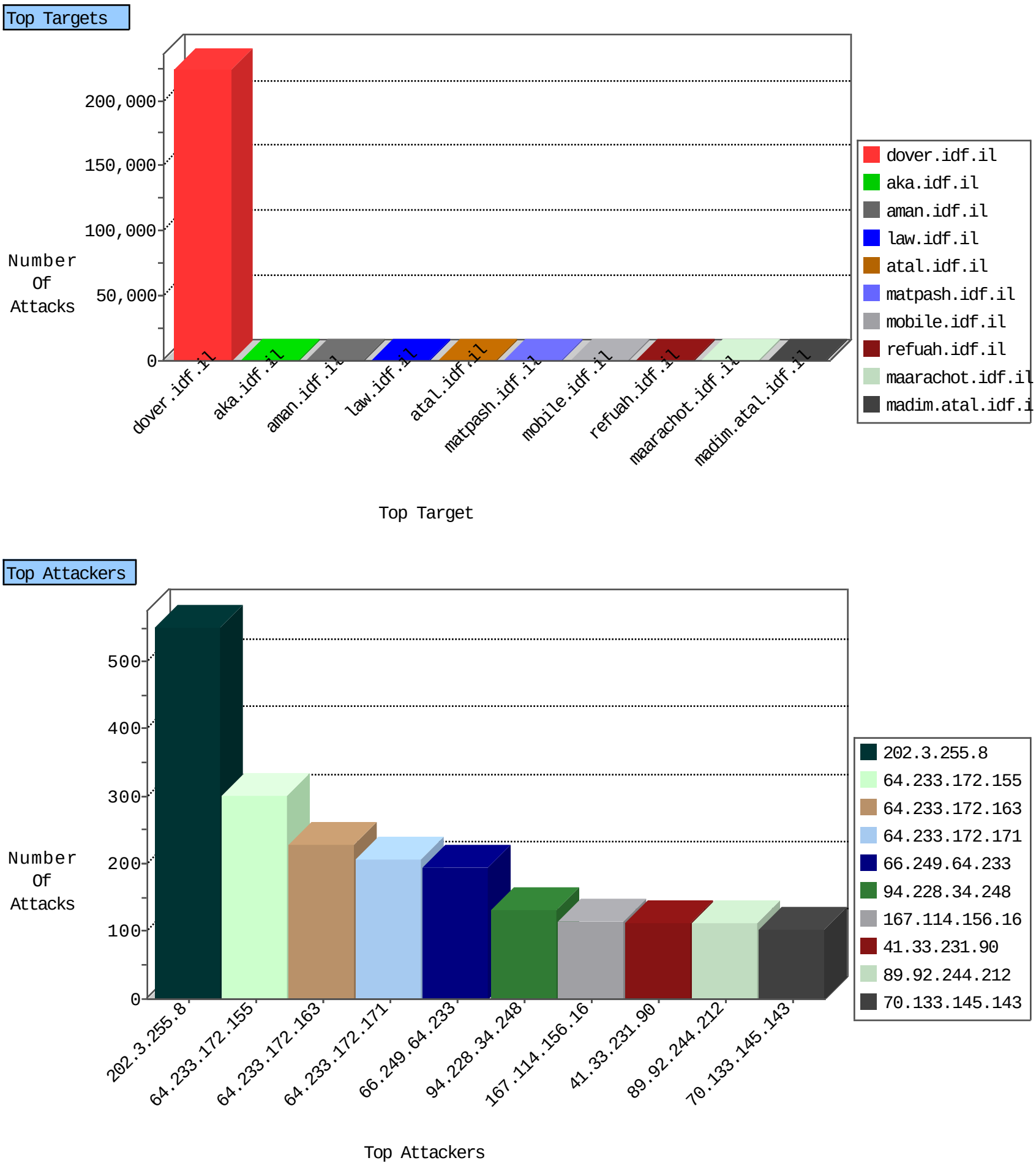
11-18-2015-02:04:00 to 11-18-2015-03:04:00

IDF Under Attack
Daily Report



11-18-2015-02:04:00 to 11-18-2015-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8208
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3427
27.19.161.118	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3199
113.104.9.101	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3174
186.207.2.89	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2545
66.249.69.42	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1583
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	932
133.46.218.63	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	473
66.249.69.101	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	381
112.242.118.3	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	329
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	234
104.173.145.82	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	210
177.29.19.58	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	169
220.191.56.40	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	156
150.55.153.45	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	156
27.220.131.12	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	121
204.151.214.58	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	114
85.250.90.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	105
150.55.0.0	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	67
180.255.71.42	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	66
113.183.207.41	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22
160.15.163.124	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
217.72.58.26	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
77.53.187.121	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
133.1.160.42	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.251.201.34	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.224.210.43	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
100.42.161.61	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.227.34.73	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.40.90.113	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.93.110.97	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
186.48.78.107	Uruguay	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
70.176.62.123	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
125.66.69.91	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.195.113.68	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.18.230.112	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
115.132.51.21	Malaysia	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
206.188.86.94	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.219.20.70	Estonia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
160.198.85.15	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.162.121.115	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
111.9.232.5	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
200.87.64.78	Bolivia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
192.232.148.86	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.186.4.22	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
139.91.92.1	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
219.3.48.3	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-18-2015-02:04:00 to 11-18-2015-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-18-2015-02:04:00 to 11-18-2015-03:04:00

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	515
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.145.30.77	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.210.6	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.222.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
130.201.104.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.51.33.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.51.110	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.22.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.202.126.57	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.171.87.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.189.173.224	147.237.76.201	Germany	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.126.23.216	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
148.248.205.28	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.106.74	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
117.207.84.49	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.43.157.90	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.202.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.93.154.216	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
74.117.209.136	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.20.165.112	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.133.9	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.170.77	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
170.67.102.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.110.93	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.213.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.196.195.39	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
167.97.48.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.64.39.101	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.34.162.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.167.174.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.76.35	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.188.115	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.183.46.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.94.14	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.16.121	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.182.91.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.228.75	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.210.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.13.3.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.174.171.104	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
134.209.102.105	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.51.46.28	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.184.120	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.140.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.85.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-18-2015-02:04:00 to 11-18-2015-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.233.172.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	301
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	228
64.233.172.171	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	208
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	132
89.92.244.212	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	112
70.133.145.143	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	103
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	76
54.159.7.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	76
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
37.26.146.252	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	69
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
177.125.245.4	Brazil	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
101.186.176.192	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
82.165.137.121	Germany	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	38
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	36
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
45.58.252.229		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
100.33.122.75	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
112.198.98.236	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
52.28.227.174	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
100.127.128.144		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	21
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
121.54.54.47	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
52.29.122.124	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
92.241.45.17	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
179.61.201.61	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
70.199.96.236	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
45.219.180.238	Uruguay	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
121.54.54.54	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
104.197.104.11	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
79.180.185.137	Israel	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
128.242.249.11	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
79.180.185.137	Israel	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
40.77.167.53	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14

11-18-2015-02:04:00 to 11-18-2015-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	2
81.218.154.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.196.50.33	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
74.208.105.30	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
62.25.16.234	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/localauth/setaccount.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.80.54.216	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.178.24.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.87.82.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
85.64.3.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.208.105.30	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
109.65.178.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.130.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/nain/sachar	Block	1
66.249.64.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8718-he/refuah.aspx	Block	1
89.138.69.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.208.105.30	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
46.31.103.89	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
115.132.51.21	Malaysia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
80.246.136.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3384.jpg	Block	1
91.196.50.33	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
74.208.105.30	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
185.25.151.159	Poland	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1

11-18-2015-02:04:00 to 11-18-2015-03:04:00