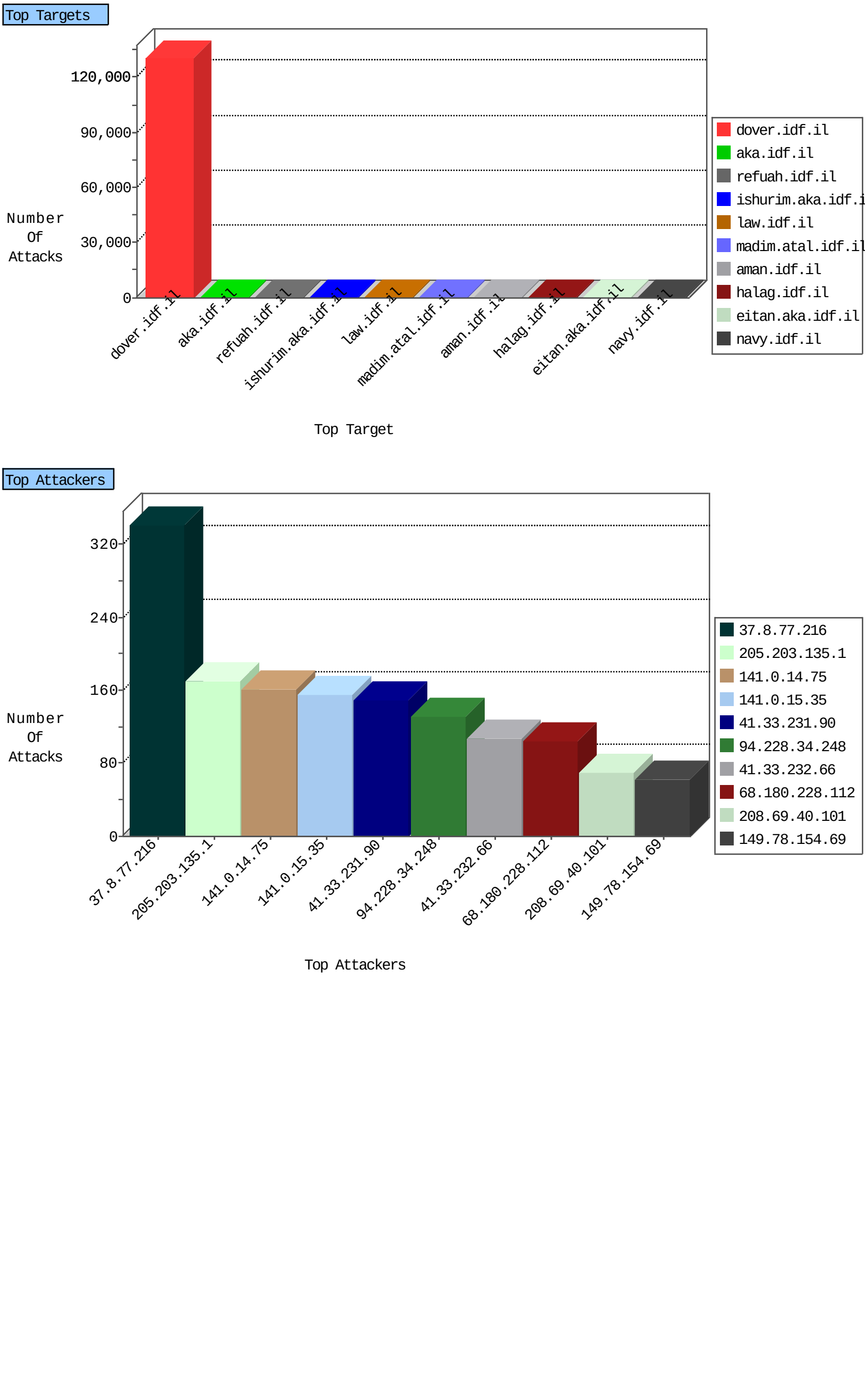
11-13-2015-07:04:04 to 11-13-2015-08:04:04

IDF Under Attack
Daily Report



11-13-2015-07:04:04 to 11-13-2015-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.32.85.33	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2520
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1988
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	465
181.17.253.125	Venezuela	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	243
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	160
183.187.240.24	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	114
118.72.184.68	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
177.252.38.125	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	75
118.219.205.62	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	68
211.109.103.120	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	54
161.10.127.52	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
203.130.214.121	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	49
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
141.0.14.75	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
74.112.18.90	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
141.0.15.35	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
89.160.32.75	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
70.71.64.100	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	3
141.0.14.75	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
66.11.188.82	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
141.0.15.35	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
93.116.227.103	Moldova, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.195.106.80	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.89.124	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
175.144.15.66	Malaysia	147.237.77.216	dover.idf.il	Invalid L4 Header Length	drop	1
64.46.27.68	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
158.75.3.19	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.33.115	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.27.196.63	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
77.111.125.26	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.52.201.21	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.19.177.86	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.11.150.112	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
68.117.102.60	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
179.1.188.22	Colombia	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
94.137.234.18	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.184.152.56	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.13.247.110	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.40.158.31	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.255.190.53	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.55.93	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
147.29.185.1	Denmark	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
82.164.31.127	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.112.18.76	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.69.68.77	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
27.100.156.61	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
130.159.204.92	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
99.247.39.3	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-13-2015-07:04:04 to 11-13-2015-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.189.171.97	Germany	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

11-13-2015-07:04:04 to 11-13-2015-08:04:04

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	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
148.248.91.106	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.192.0.20	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.223.71.75	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.41.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.48.58.187	147.237.77.216	United Arab Emirates	dover.idf.il	portscan: TCP Distributed Portscan	1
167.28.121.55	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.128.87	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.189.10.122	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.179.74	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.2.109	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.133.70	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
179.181.142.2	147.237.76.38	Brazil	e.e.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
134.172.165.28	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.69.8	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.55.74	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.60.107	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.96.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.36.66	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.172.154	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.49.87	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.214.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.207.42	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.145.106	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.179.54	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.144.1.47	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.158.47	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.64.111.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.223.238.55	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.174.29	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.45.12	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.151.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.243.14	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.187.227.1	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.227.77	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.218.208.65	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.71.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.158.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.254.3	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.82.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.228.124	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.59.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.106.173.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.97.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.43.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.138.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.31.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.56.93	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.114.49	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-13-2015-07:04:04 to 11-13-2015-08:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.8.77.216	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	342
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	171
141.0.15.35	Europe	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	132
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
141.0.14.75	Europe	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	119
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
207.46.13.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
62.210.181.90	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
121.54.58.130	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
207.46.13.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
141.0.14.75	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
157.55.39.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
207.46.13.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
79.181.61.100	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
198.1.101.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.146.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	22
176.13.18.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
99.224.147.123	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
208.54.85.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
204.93.154.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.13.20.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
37.26.146.161	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.20.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.51.7		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.117.9.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
80.246.136.210	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
104.131.200.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12

11-13-2015-07:04:04 to 11-13-2015-08:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.32.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
37.142.184.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.12.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.39.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.78.231.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.68.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.83	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.195.143	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.121	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.150.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3350.jpg	Block	1
157.55.39.141	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.1.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.121	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/general...067&docid=31516	Block	1
109.66.217.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
176.12.142.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.130.196	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.120.229.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
2.54.160.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.100.26.229	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
109.186.47.95	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Malformed URL zzzzzzz=ed810aedzzzzzzz_ed810aed	Block	1
82.166.140.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1217-he/refuah.aspx&arubalp=9539b244-d465-44bf-ae7a-460a468acd	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
31.154.94.9	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
216.218.206.68	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
74.82.47.4	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 447183120.; in URL zzzzzzz=ed810aedzzzzzzz_ed810aed	Block	1
207.46.13.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-22583-he	Block	1
85.65.200.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

11-13-2015-07:04:04 to 11-13-2015-08:04:04