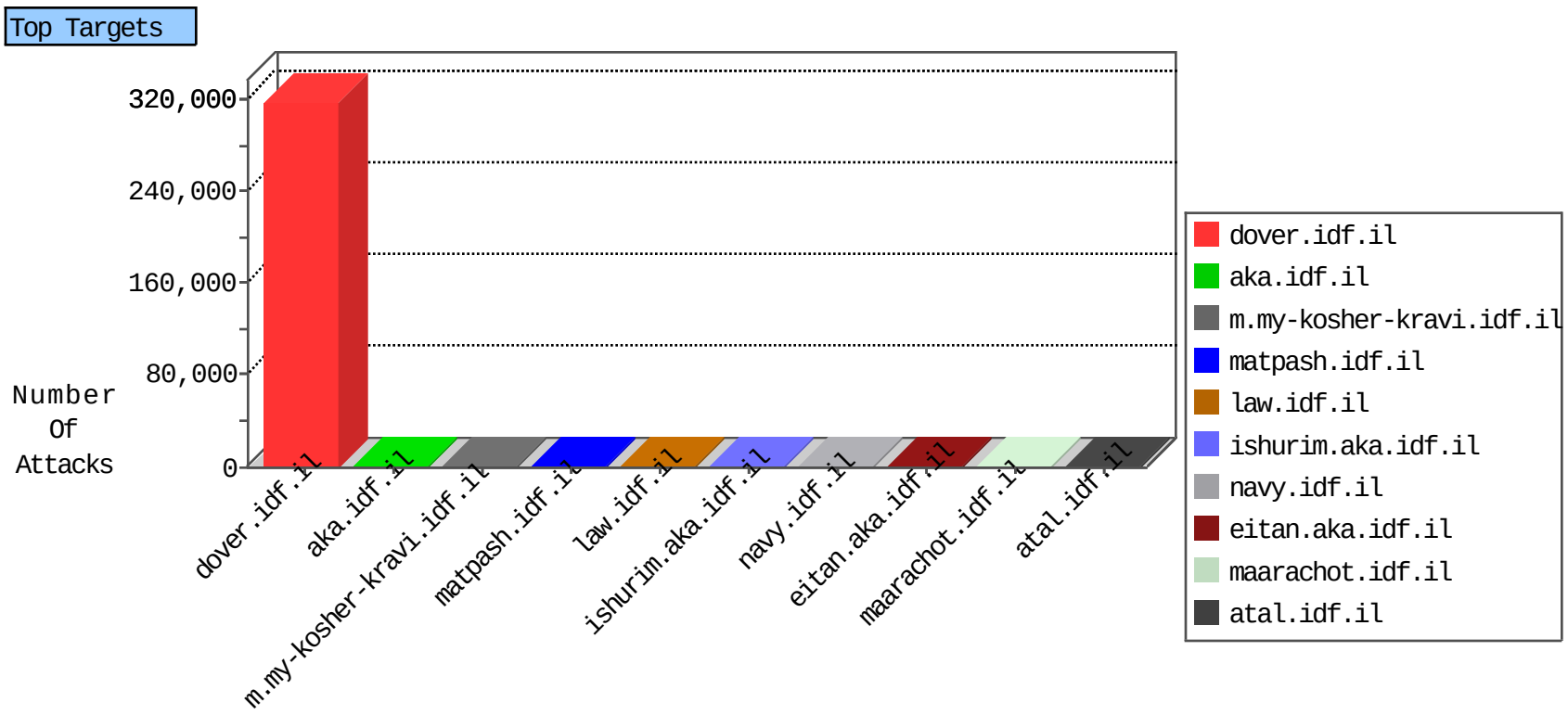
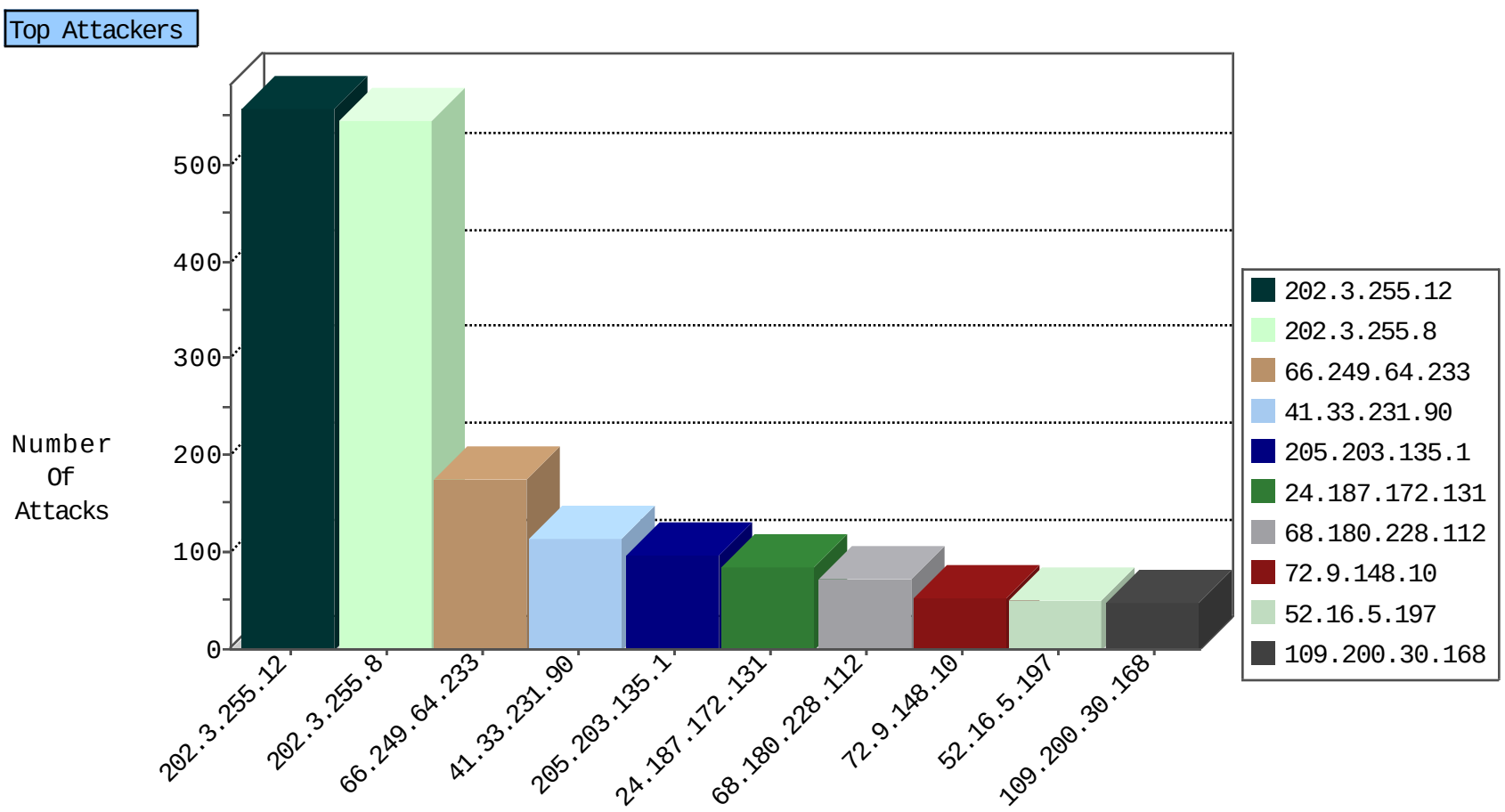
11-20-2015-05:04:09 to 11-20-2015-06:04:09

IDF Under Attack Daily Report





11-20-2015-05:04:09 to 11-20-2015-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
24.98.41.211	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5164
209.129.115.58	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4602
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1166
220.181.108.141	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	329
204.93.154.216	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	11
94.255.218.98	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
173.178.156.40	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
198.217.117.75	Canada	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
206.214.243.43	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
115.230.124.164	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
58.176.170.17	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
97.85.36.6	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
78.31.158.86	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.200.83.48	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.61.63.114	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
180.150.54.7	Australia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.151.236.35	Slovenia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.228.201.60	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
71.15.33.30	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
67.231.119.40	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
176.96.152.96	Austria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.209.121	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
92.39.155.113	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.179.192.10	Netherlands	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.100.115.108	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.6.233.103	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.90.104	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
158.193.227.97	Slovakia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.98.110	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
119.162.32.103	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.115.45.12	Kazakstan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.145.115.115	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
73.149.243.25	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.90.109.125	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
59.35.85.0	China	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
95.180.153.35	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.246.66.103	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.76.156.87	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
222.124.4.14	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.170.208.36	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
180.97.106.36	China	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
67.20.249.50	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.228.72.69	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
12.216.64.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.208.71.39	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.52.39.15	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.75.192.73	Switzerland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.225.44.35	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.234.248.113	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-20-2015-05:04:09 to 11-20-2015-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.94	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-20-2015-05:04:09 to 11-20-2015-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	522
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	508
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.81	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
157.232.78.65	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.174.150.164	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
199.165.53.18	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.167.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.70.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.194.214.111	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.189.24.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.242.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.174.150.164	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
199.101.186.134	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
134.172.10.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.199.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.224.29	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
205.203.253.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.179.117	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.183.60.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.199.89	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.145.124	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
50.252.197.194	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 2048	1
67.211.221.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.106.221.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.43.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.23.80	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.13.0.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
121.46.124.119	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.126.103	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.85.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
204.106.173.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.42.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.251.125	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.235.254.181	147.237.72.217	Turkey	e.idf.il	ET SCAN NMAP -sS window 3072	1
148.178.69.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
195.5.161.57	147.237.77.216	Moldova, Republic of	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.1.64	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.77.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.107.85	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.208.87	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
186.190.230.92	147.237.77.216	Panama	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.194.88	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.224.127	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.255.63	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.124.22	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
201.235.215.254	147.237.72.166	Argentina	aka.idf.il	ET SCAN NMAP -sS window 2048	1
148.105.77.110	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-20-2015-05:04:09 to 11-20-2015-06:04:09

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.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	122
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
24.187.172.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
50.87.144.145	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
209.129.115.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
5.45.203.204	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
107.170.16.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
72.28.218.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	28
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
71.168.187.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.80.46.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
71.236.164.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
88.198.157.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
207.46.13.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
208.54.80.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
71.59.110.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.13.4.199	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.131.200.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
97.74.24.187	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
204.93.154.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.166.186.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
62.45.94.123	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.231.189.127	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
87.203.103.152	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.4.199	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	10
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.4.199	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
2.54.158.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.111	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.230.67.73	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
176.13.14.227	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
204.93.154.216	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.52.241	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 2.54.52.241	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/links.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
178.63.96.242	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	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/7/3137.doc	Block	1
204.93.154.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
2.54.52.241	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
185.13.194.61	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
80.178.24.108	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19754-he/dover.aspx	Block	1
207.46.13.4	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.4	Block	1
2.54.158.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	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
65.78.117.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.52.241	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
81.144.138.34	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	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
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org	Block	1
40.77.167.11	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
178.63.96.242	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 178.63.96.242	Block	1
66.249.73.197	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/284.pdf	Block	1

11-20-2015-05:04:09 to 11-20-2015-06:04:09