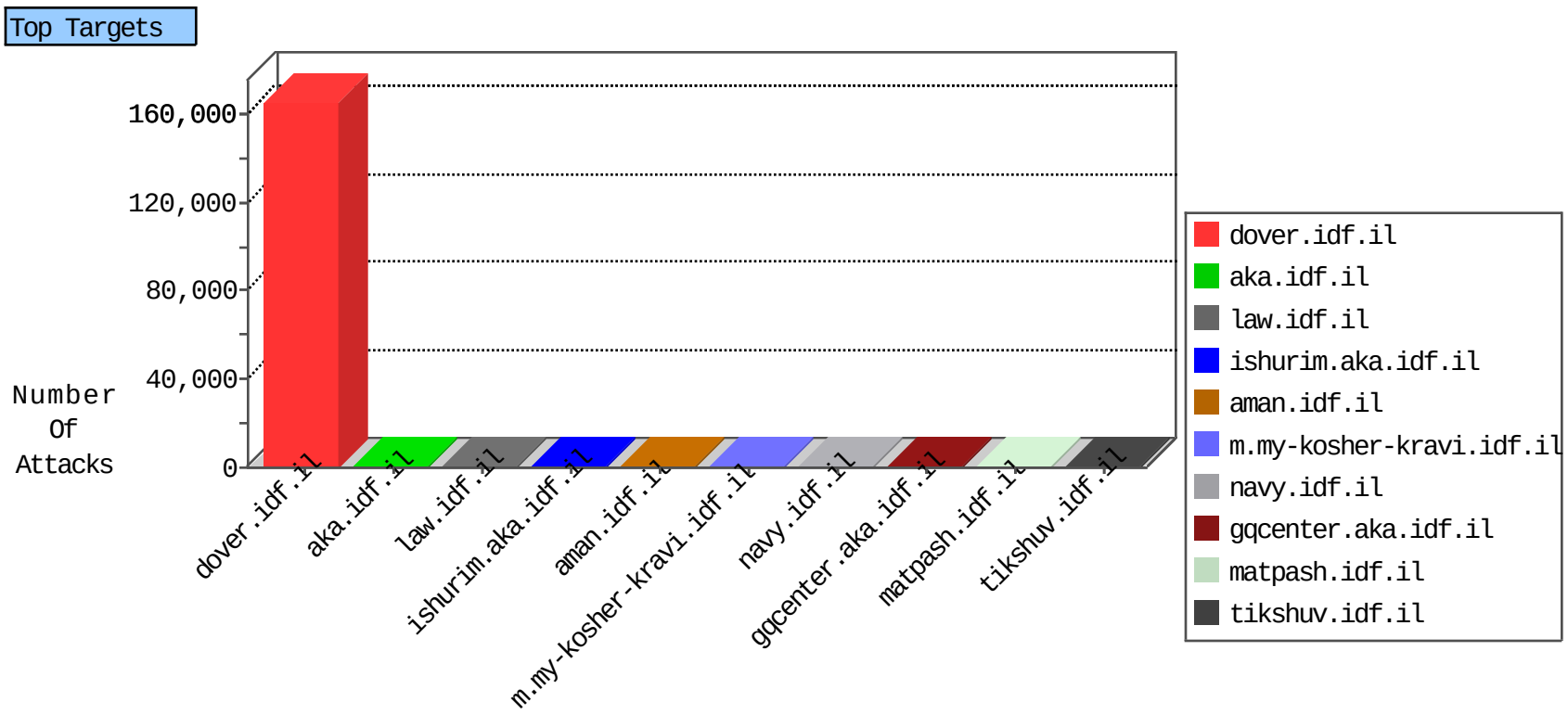
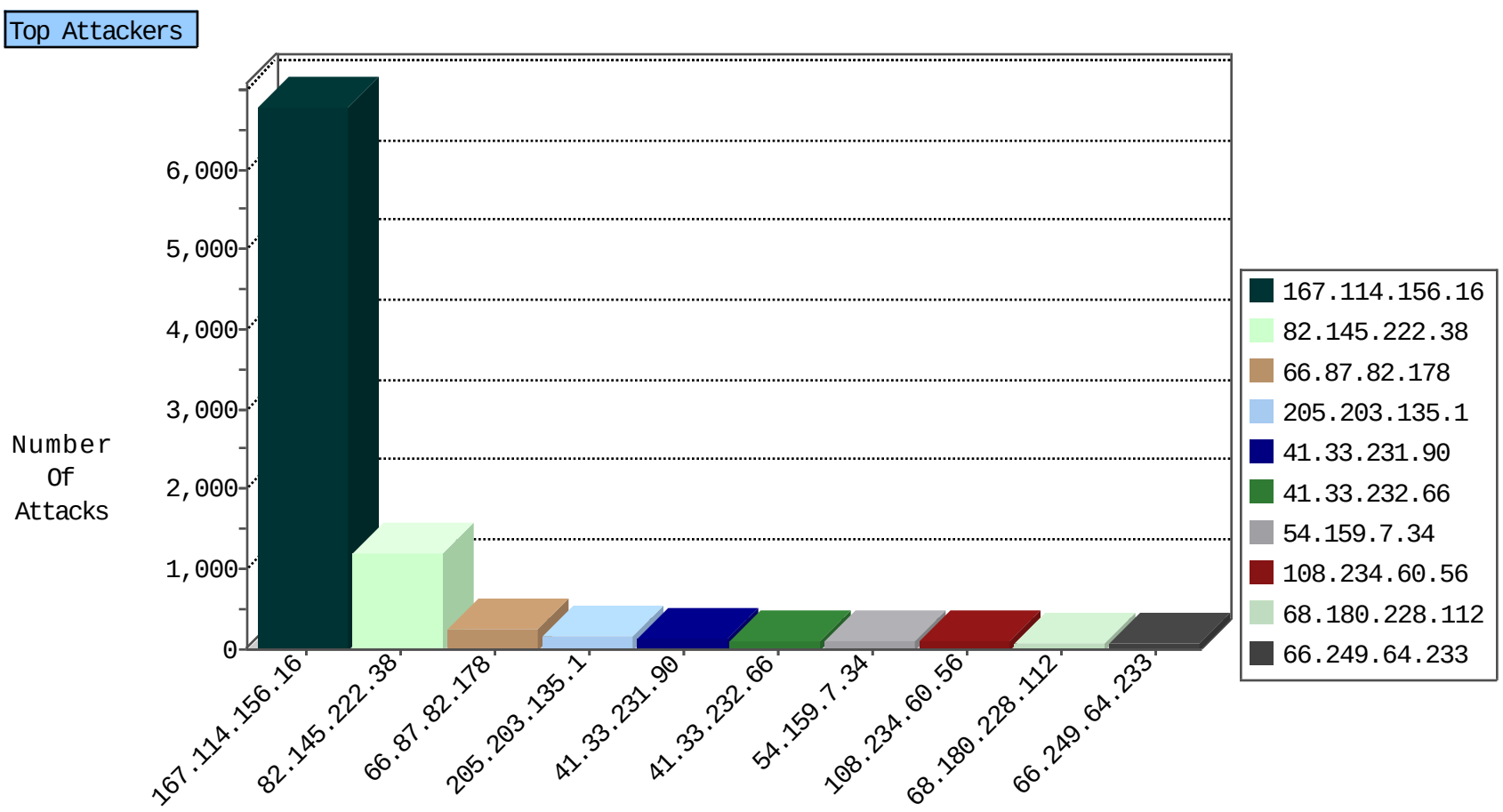
11-15-2015-02:04:09 to 11-15-2015-03:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-15-2015-02:04:09 to 11-15-2015-03:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
27.96.206.6	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2772
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1332
220.181.108.160	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	300
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	224
27.237.171.82	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	86
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	66
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	9
79.176.39.96	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
82.145.222.38	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
24.105.193.35	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
203.25.98.3	Australia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
63.248.132.102	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
69.31.212.9	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
99.53.184.1	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.104.116.40	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.51.52	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.12.174.9	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
47.60.207.95	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.139.101.2	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.138.81	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.16.69.30	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
114.158.90.118	Japan	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
72.215.200.4	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.141.97	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.114.176.31	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.145.115.62	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.175.71.40	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.49.12.37	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.98.39.17	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
190.11.152.26	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.0.62.5	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.103.81	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.230.128.119	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
131.215.195.33	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
103.31.242.35	Hong Kong	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	1
69.170.203.37	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.160.30.105	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.131.125	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.23.61.16	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
47.60.237.71	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.169.167.17	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.211.141.116	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.168.73.102	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.58.40.72	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
8.30.180.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1

11-15-2015-02:04:09 to 11-15-2015-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.202	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	4
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.201	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.233	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-15-2015-02:04:09 to 11-15-2015-03:04:09

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
157.232.68.14	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.64	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.178	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
134.172.196.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.213.92	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.67.61	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.50.27	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.54.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.61.159.221	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.34.138.27	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.99.30	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.199.34	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.212.125.24	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
213.109.214.105	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.136.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.241.91	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.32.16.50	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
134.127.166.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.33.17	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.206.200.109	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
210.117.121.60	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
140.170.183.18	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.219.121.45	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.139.9	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.119.92	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.197.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.186.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.22.234.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.15.32	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.171.70.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.57.13	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.254.91	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.42.141.48	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.235.35	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.77.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.212.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.72.105	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.254.29	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.255.4	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.211.23	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.196.75.95	147.237.72.166	France	aka.idf.il	ET SCAN NMAP -sS window 1024	1
204.236.30.12	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.160.28	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.46.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.67	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
116.199.143.76	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.135.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.159.62	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-15-2015-02:04:09 to 11-15-2015-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6729
82.145.222.38	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1200
66.87.82.178	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	263
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	153
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	108
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
54.159.7.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
108.234.60.56	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	95
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	83
54.224.21.23	United States	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
84.94.15.200	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
66.87.31.111	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
188.96.94.17	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
174.3.53.187	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
197.36.38.74	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
113.5.80.71	China	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	43
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	42
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
222.163.195.6	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
62.44.135.129	Denmark	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
201.141.105.177	Mexico	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
52.29.46.119	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
5.196.75.168	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
64.46.23.242	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
217.66.251.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
157.55.39.217	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
209.126.117.15	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
5.196.75.168	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
178.63.55.202	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
207.46.13.38	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
207.46.13.156	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
157.55.39.93	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
175.32.145.204	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
157.55.39.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
99.20.182.117	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16

11-15-2015-02:04:09 to 11-15-2015-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	10
190.142.122.201	Venezuela	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.95	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
208.115.111.74	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/news/null	Block	1
84.94.174.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.67	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/undefined	Block	1
36.248.163.105	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
192.99.16.165	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
72.190.74.42	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 72.190.74.42 (Open Mode)	None	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16985-he/dover.aspx	Block	1
157.55.39.83	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
64.19.78.242	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
207.46.13.148	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
72.190.74.42	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	1
159.203.132.43	United States	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/112324.pdf	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.230	Block	1
207.46.13.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	Block	1
79.176.200.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
176.12.142.237	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.142.237	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.159	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/4170.pdf×€×ŸÂ¿Â½×€Â¾×?Â?×€Â¼×€Â¾×?×ŸÂ¿Â½×?×ŸÂ¿Â½×€Âµ×?×ŸÂ¿Â½×?×ŸÂ¿Â½	Block	1
80.178.157.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-15-2015-02:04:09 to 11-15-2015-03:04:09