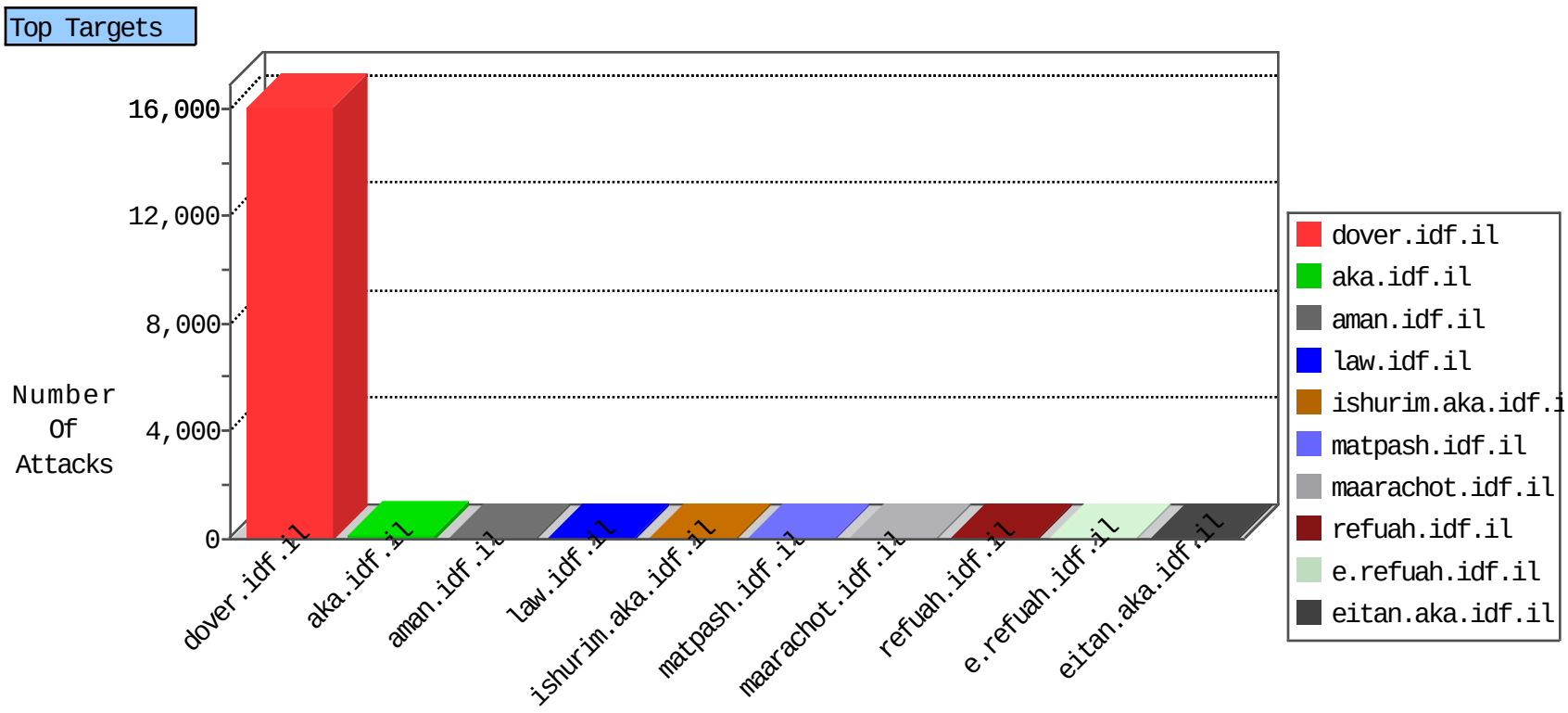
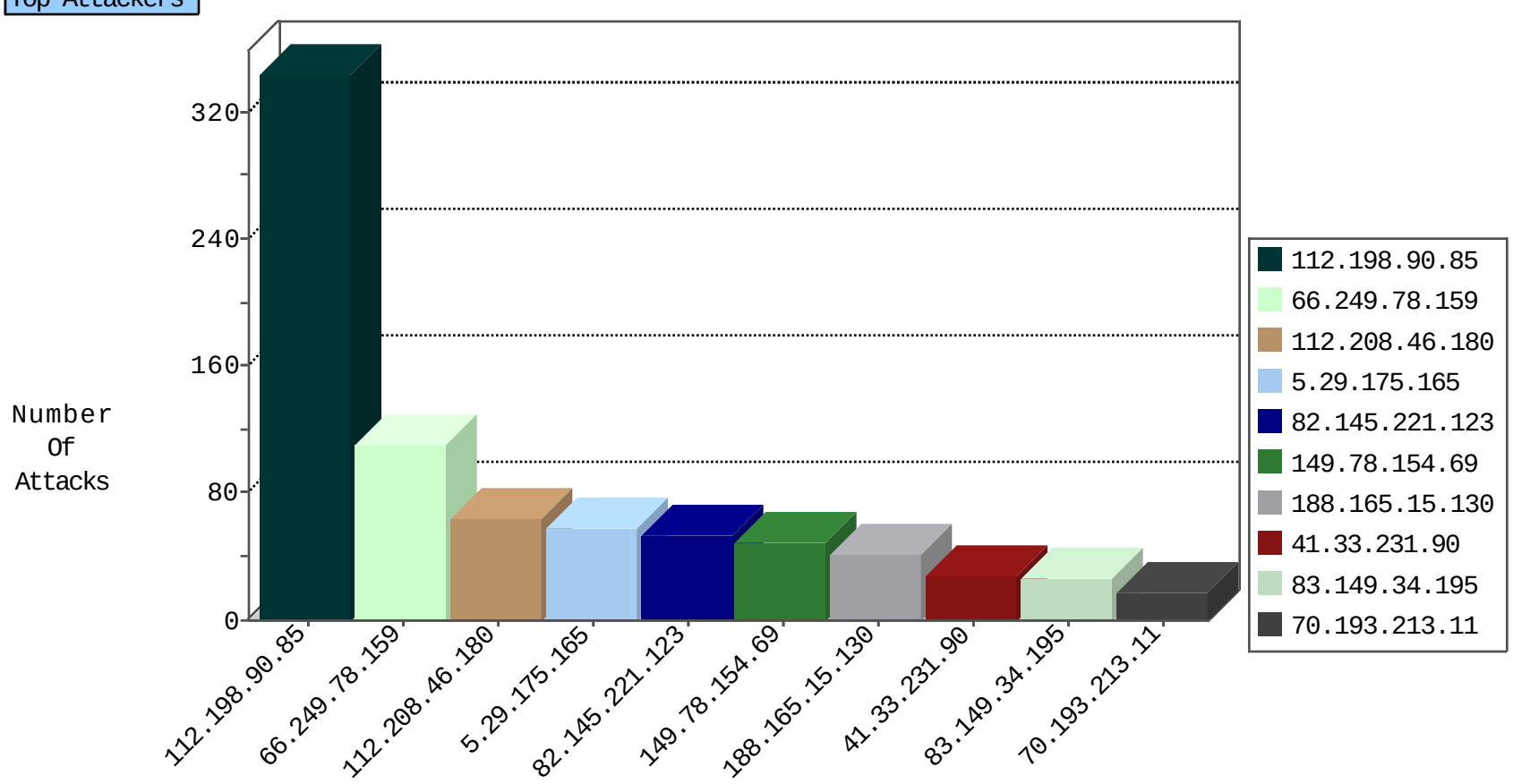
11-14-2015-07:04:04 to 11-14-2015-08:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-14-2015-07:04:04 to 11-14-2015-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	172
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	17
89.239.1.102	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
72.46.204.55	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
99.241.47.102	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.177.111.61	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.30.147.2	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.145.115.67	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.9.149.58	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.144.55	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
195.93.174.43	Austria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.204.233.88	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.205.95	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
68.188.239.118	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.88.101.50	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.65.180.61	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.209.10.40	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.97.198.51	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.11.152.37	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.31.28.123	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
78.136.77.56	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
151.177.22.124	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.93.119.115	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.107.153.27	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.162.20.40	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.27.127	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.30.224.70	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
206.214.151.8	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.205.147.107	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.39.106.18	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.42.77.35	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.172.42	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.107.140.107	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.215.86	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.187.65	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.209.60.61	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.40.2	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
192.222.194.99	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.60.247.126	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.78.148.15	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
217.191.134.74	Germany	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
213.182.250.13	Austria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.29.111.103	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.162.209.92	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
177.91.159.21	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.68.2	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.25.92.3	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.46.15.108	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.21.212.105	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.132.7	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-14-2015-07:04:04 to 11-14-2015-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.36	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.201	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.147	Italy	147.237.0.34	tikshuv.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
188.165.15.202	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.124	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-14-2015-07:04:04 to 11-14-2015-08:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
67.211.212.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.243.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.61.113	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.45.32.3	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.94.4	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.189.9.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.131.34.25	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.187.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.96.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.62.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.111.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
194.44.4.37	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.76.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.115.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.213.41	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.118.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.208.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.22.202.3	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.184.44	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.236.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
121.46.105.36	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.115.117	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.191.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.252.66	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
220.245.240.26	147.237.0.35	Australia	akaws.idf.il	ET SCAN NMAP -f -sS	1
170.113.89.114	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.185.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.137.14.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.4.97	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.47.105	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.94.209.35	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.171.73.50	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.54.80	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.5.50	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.108.132.58	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
159.223.81.40	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.12.36	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.87.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
201.7.221.87	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.181.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.168.23.93	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.112.83.117	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.225.28	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
8.37.225.191	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
159.223.50.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.229.100	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-14-2015-07:04:04 to 11-14-2015-08:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
112.198.90.85	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	344
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
112.208.46.180	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
82.145.221.123	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	41
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
83.149.34.195	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
210.101.133.12	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	14
188.165.15.233	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
94.230.86.160	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.15.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
70.193.213.11	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.125.83.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
70.193.213.11	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.24.37		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.52.39.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
108.201.230.0	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.15.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop		drop	4
64.233.172.222	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
128.232.110.28	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
40.77.167.45	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.233.172.214	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.34	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.94.163.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.172.131.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
93.172.131.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.186.145.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
157.55.39.25	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.43	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
159.253.145.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.9	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

11-14-2015-07:04:04 to 11-14-2015-08:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
49.144.88.116	Philippines	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 49.144.88.116	Block	2
84.94.207.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
173.236.176.101	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.67.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9692-he/refuah.aspx	Block	1
40.77.167.45	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/	Block	1
207.46.13.9	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21050-h	Block	1
49.144.88.116	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/	Block	1
185.80.220.181		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.73.228	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/hahnasatagalimaza.aspx	Block	1
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/forgotpassword.aspx	Block	1
66.249.64.165	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
188.138.17.205	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
49.144.88.116	Philippines	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
207.46.13.163	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/home/default.aspx	Block	1
27.153.204.159	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
193.182.144.142	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
49.144.88.116	Philippines	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 49.144.88.116	Block	1
210.101.133.12	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.172	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/recruitinformation	Block	1
66.249.66.90	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
37.247.54.2	Italy	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
204.236.235.245	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1

11-14-2015-07:04:04 to 11-14-2015-08:04:04