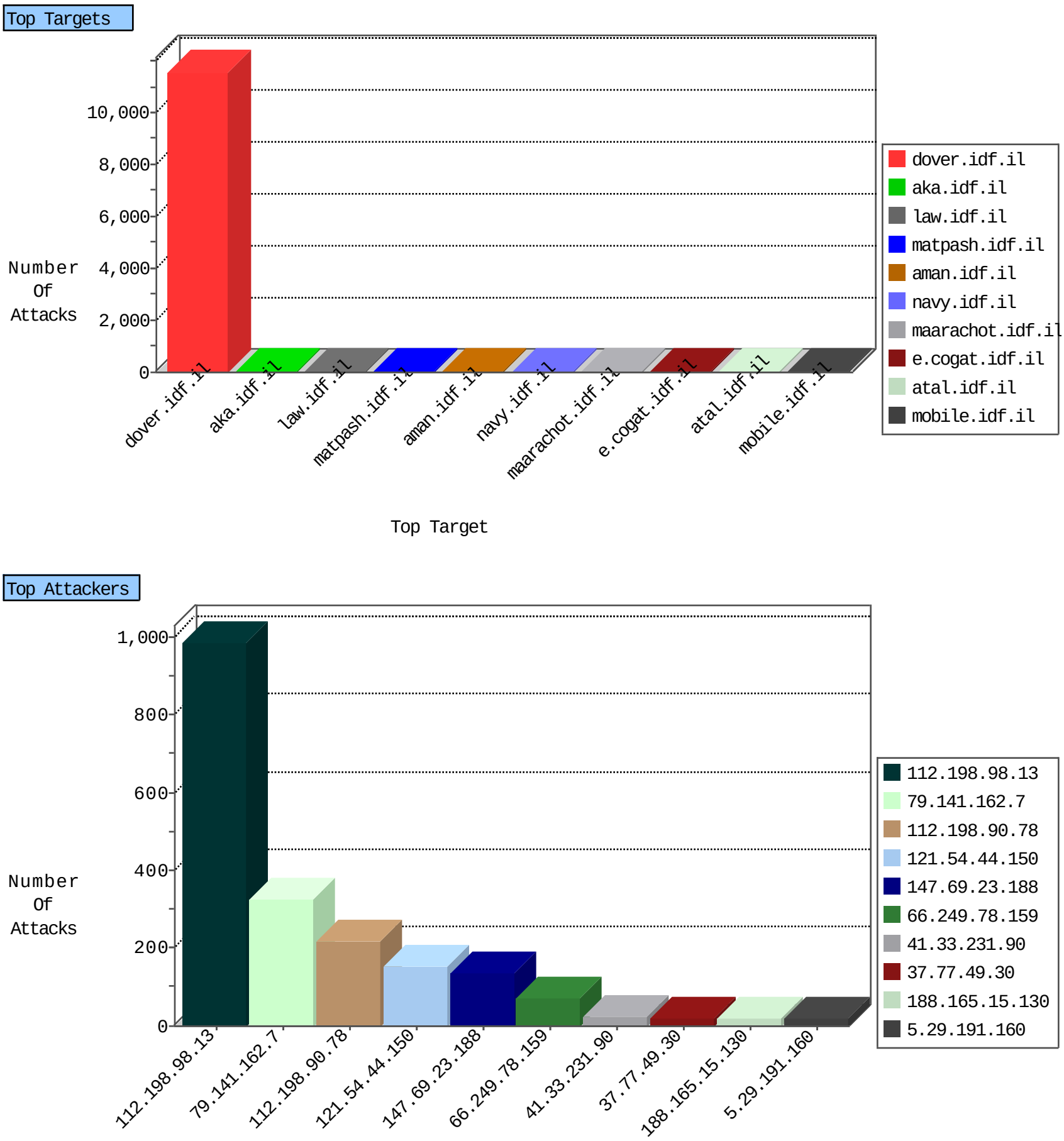
11-14-2015-05:04:08 to 11-14-2015-06:04:08

IDF Under Attack
Daily Report



11-14-2015-05:04:08 to 11-14-2015-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	534
37.77.49.30	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	232
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	173
64.194.160.103	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.74.50.96	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.215.228.16	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
81.170.178.8	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
47.60.177.100	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
112.175.63.34	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.148.125.62	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
96.30.239.117	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.214.185.101	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.80.99.64	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.31.212.92	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.73.21.44	Chile	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
23.91.233.43	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.195.54	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.160.75.84	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.64.14	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.90.166.33	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.144.86	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	DOS-Tool-SwitchbladG	dest-reset	1
84.20.64.54	Albania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
77.239.140.98	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.189.212.73	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.33.56.7	Ukraine	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
105.235.106.64	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.239.125	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.229.108	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.19.138.85	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.186.49.46	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.131.21	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
92.245.144.17	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
67.80.64.100	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.19.47.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
183.78.186.117	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.24.237.40	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
81.191.20.67	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
50.67.28.90	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
121.210.251.124	Australia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.45.110.11	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
99.226.108.126	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
75.172.157.83	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.26.100.62	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.67.10.71	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
201.77.116.119	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.52.217.68	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.200.67	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.176.144.13	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.89.42	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-14-2015-05:04:08 to 11-14-2015-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	4
36.80.10.28	Indonesia	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.202	France	147.237.76.30	himush.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
188.165.15.36	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-14-2015-05:04:08 to 11-14-2015-06:04:08

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
37.77.49.30	147.237.77.216	Iraq	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
170.106.62.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.62.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.36.107	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.0.228.102	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
130.201.120.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.183.202.87	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.196.119	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.125.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.181.76.183	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
204.93.154.216	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.54	147.237.8.27	Moldova, Republic of	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
63.141.52.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.187.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
37.77.49.30	147.237.77.216	Iraq	dover.idf.il	portscan: TCP Distributed Portscan	1
167.97.194.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.6.71.154	147.237.8.45	Poland	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
147.69.23.188	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
140.170.53.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.14.168.236	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.199.184.112	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.227.95.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.173.85	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.175.168.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.91.124	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.48.195	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.2	147.237.77.178		e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

11-14-2015-05:04:08 to 11-14-2015-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
112.198.98.13	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	988
112.198.90.78	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	216
147.69.23.188	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	120
121.54.44.150	Philippines	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	79
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
188.165.15.233	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	16
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
5.29.191.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.141.162.7	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.29.191.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	7
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
147.69.23.188	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
109.186.173.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
121.54.44.168	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.69.23.188	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.26	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.150	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
75.126.221.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
147.69.23.188	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	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
176.228.217.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.29.191.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
5.102.227.214	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.227.214	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
27.109.83.50	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.71.71.89	Armenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.121.84.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.121.84.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.194.164.85	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.210.132.11	France	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
62.210.209.237	France	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
67.49.212.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
70.82.163.75	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.59.205.111	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
76.95.130.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
88.83.151.68	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
121.246.35.113	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

11-14-2015-05:04:08 to 11-14-2015-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.141.162.7	Ireland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	317
121.54.44.150	Philippines	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 121.54.44.150	Block	73
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
84.111.232.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
121.54.44.150	Philippines	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
74.208.105.30	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
157.55.39.242	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
157.55.39.150	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
74.208.105.30	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=1995de47kkkkkkk_1995de47	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
157.55.39.155	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/default.aspx	Block	1
74.208.105.30	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
186.26.115.67	Costa Rica	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 186.26.115.67 (Open Mode)	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-ar/cogat.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/faq/pages/default.aspx	Block	1
77.237.138.51	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
147.69.23.188	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/sitemap.xml	Block	1
74.208.105.30	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
157.55.39.242	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.242	Block	1
66.249.67.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1

11-14-2015-05:04:08 to 11-14-2015-06:04:08