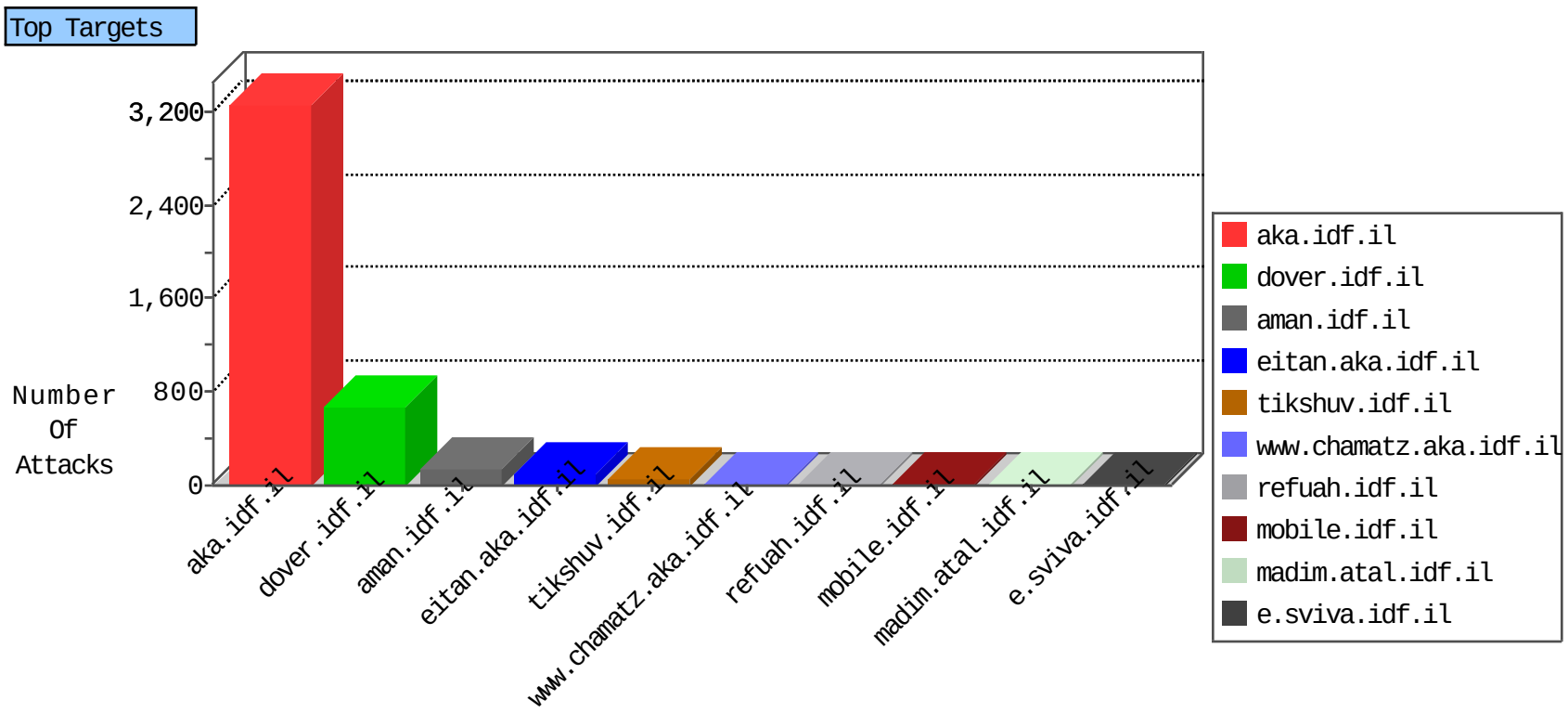
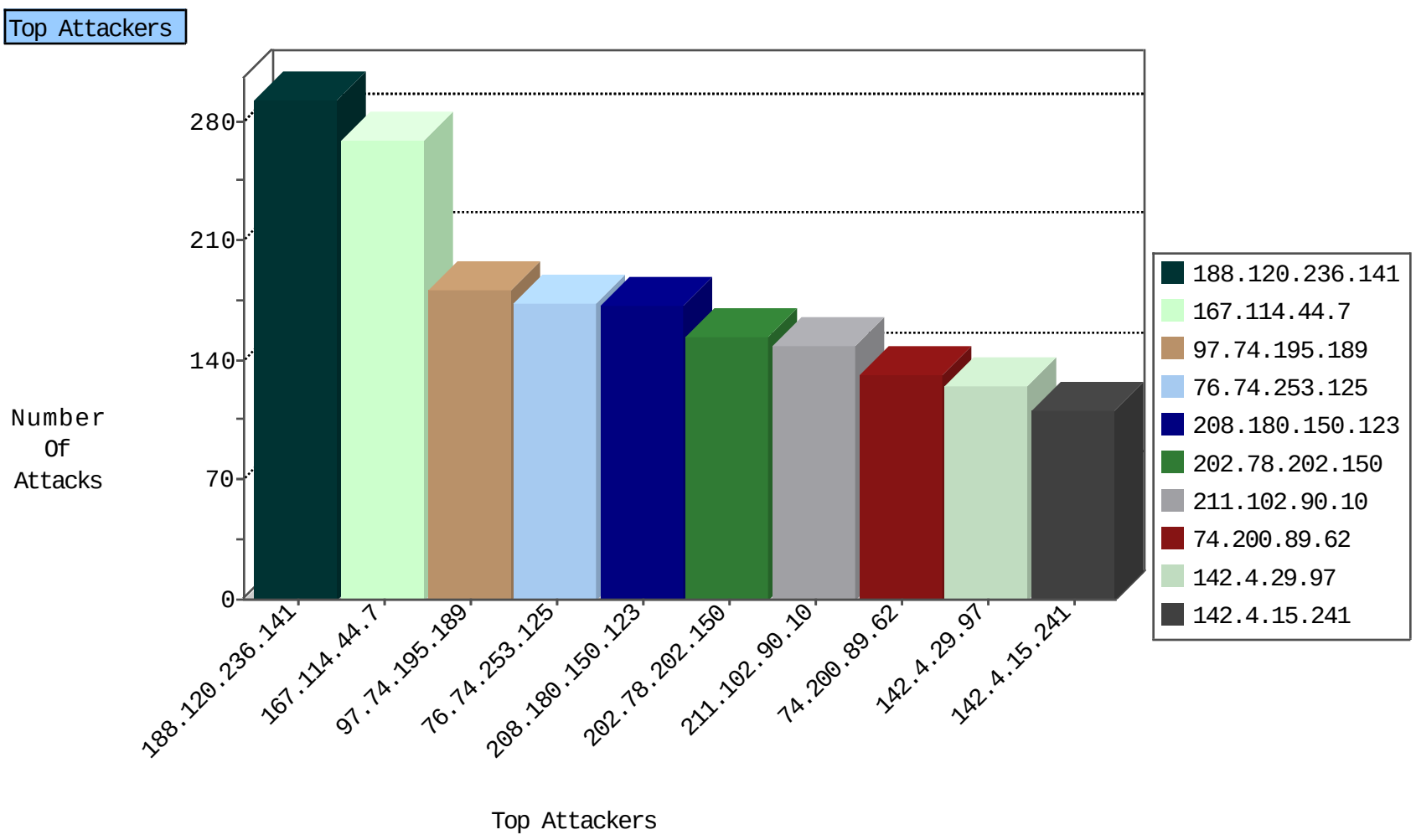
04-27-2016-07:04:09 to 04-27-2016-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-27-2016-07:04:09 to 04-27-2016-08:04:09

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	2380
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1734
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	19
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
80.82.78.38	Netherlands	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
142.4.20.33	United States	147.237.72.156	aman.idf.il	SYN Flood delete reset	drop	1
121.127.7.48	Philippines	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
167.114.44.7	Canada	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
80.82.78.38	Netherlands	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
121.127.7.49	Philippines	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
66.180.192.225	United States	147.237.72.156	aman.idf.il	SYN Flood delete reset	drop	1
202.78.202.150	Indonesia	147.237.72.156	aman.idf.il	SYN Flood delete reset	drop	1
121.127.7.51	Philippines	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
116.113.69.241	China	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-27-2016-07:04:09 to 04-27-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.47.2.10	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.234.228.90	Germany	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-27-2016-07:04:09 to 04-27-2016-08:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
96.47.2.10	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.234.228.90	147.237.0.34	Germany	tikshuv.idf.il	SQL Injection - Select From	4
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
202.170.80.40	147.237.8.14	Mongolia	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
128.199.135.89	147.237.72.156	Singapore	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.190.180	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.241.178	147.237.72.156	Singapore	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.108.187	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.82.78.38	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.138.159	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

04-27-2016-07:04:09 to 04-27-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.120.236.141	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	293
167.114.44.7	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	268
97.74.195.189	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	182
76.74.253.125	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	174
208.180.150.123	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	172
211.102.90.10	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	143
74.200.89.62	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	131
142.4.29.97	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	125
142.4.15.241	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	111
202.78.202.150	Indonesia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	108
50.56.186.113	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	93
198.1.100.140	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	92
219.94.128.98	Japan	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	91
68.4.170.129	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
203.150.20.122	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	87
95.211.156.239	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	87
195.154.176.92	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	83
188.165.211.59	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	79
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
184.73.171.53	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	60
219.94.129.22	Japan	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	57
41.44.99.119	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
51.255.99.120	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	53
23.106.239.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
119.81.69.138	Singapore	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	51
23.106.166.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
91.108.88.155	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
188.165.222.30	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
184.106.204.184	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
209.35.112.222	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
91.109.30.73	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	39
80.67.17.34	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
202.22.156.147	New Caledonia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
202.78.202.150	Indonesia	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	28
108.228.146.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
91.121.146.124	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
50.56.227.251	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
173.201.216.75	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
173.203.218.23	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
178.211.45.122	Turkey	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
37.122.210.162	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
50.63.86.209	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
200.75.19.157	Chile	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
37.26.146.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
64.65.32.22	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
72.177.51.46	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
210.224.185.85	Japan	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
70.187.73.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.132.249	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	8
46.116.22.157	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
91.108.88.226	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	1
176.13.13.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	1
45.244.28.59	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.72.215.18	United Kingdom	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/index.php	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3098.jpg	Block	1
5.39.222.159	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/16838.jpg	Block	1
69.137.183.128	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
111.85.179.73	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/modiin/default.aspx	Block	1
66.249.66.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1131-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
202.78.202.150	Indonesia	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.183.200.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.174.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
141.212.122.161	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.69.243	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/general.aspx	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
80.82.78.38	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
66.249.66.44	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
151.80.31.162	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
45.244.28.59	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1