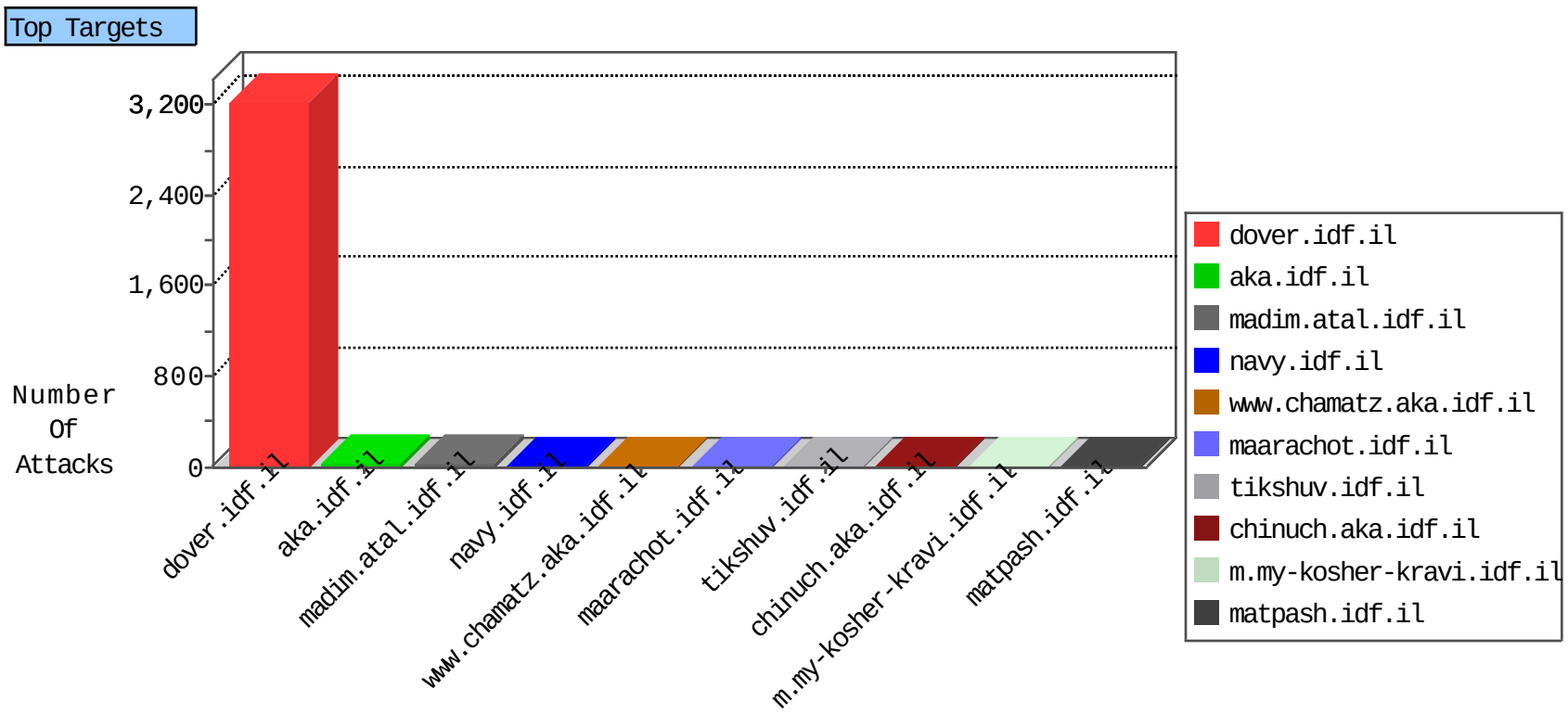
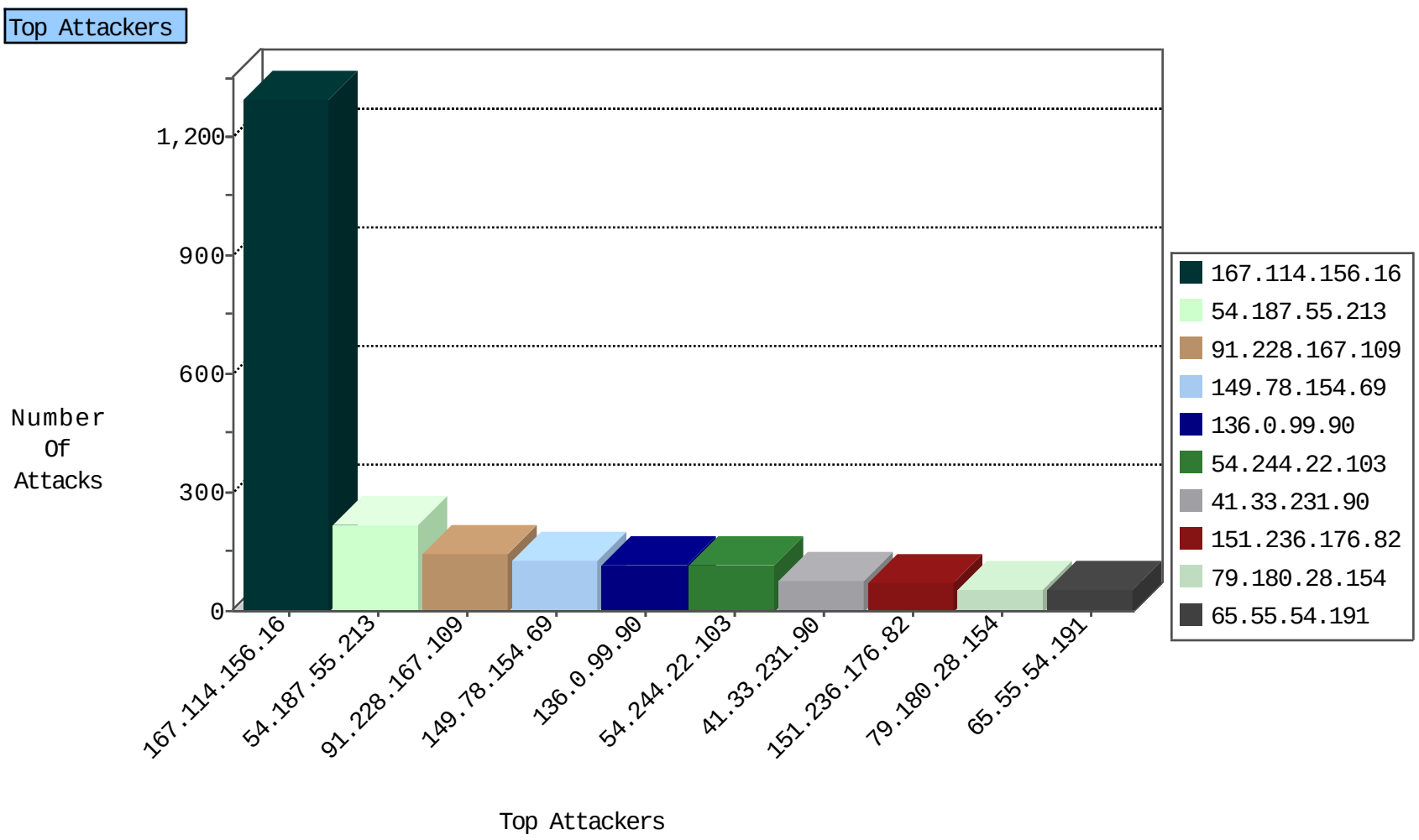
11-06-2015-06:04:05 to 11-06-2015-07:04:05

IDF Under Attack Daily Report





11-06-2015-06:04:05 to 11-06-2015-07:04:05

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	DOS-Tool-SwitchbladG	dest-reset	2186
176.13.19.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
84.109.12.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
95.185.91.24	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
31.210.186.148	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.121.15.72	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
59.148.91.18	Hong Kong	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

11-06-2015-06:04:05 to 11-06-2015-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-06-2015-06:04:05 to 11-06-2015-07:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.191	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
188.138.9.51	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
112.175.228.199	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1

11-06-2015-06:04:05 to 11-06-2015-07:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	220
91.228.167.109	Slovakia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	143
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	130
136.0.99.90	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	116
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	115
151.236.176.82	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	73
79.180.28.154	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
65.55.54.191	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
176.28.46.163	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
110.174.76.65	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
174.44.100.56	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.249.69.26	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
64.46.23.242	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
157.55.39.181	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	21
66.249.69.34	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
157.55.39.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
188.48.215.144	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
66.249.69.42	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.115	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
149.88.81.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
98.150.154.247	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
176.13.19.206	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
50.116.28.209	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
95.185.91.24	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
98.216.106.141	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
79.182.181.253	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
125.212.124.136	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
176.12.138.18	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
208.184.112.75	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	8
68.184.245.199	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
131.253.25.156	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.249.69.26	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
2.54.29.137	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
198.58.102.96	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
187.149.197.237	Mexico	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 187.149.197.237	Block	4
187.149.197.237	Mexico	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.85.132	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
207.46.13.27	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	2
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.25.40	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
162.243.215.132	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.215.132	Block	2
66.249.65.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71652-he/maarachot.aspx	Block	1
207.46.13.3	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.79.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 66.249.79.20	Block	1
66.249.65.25	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
182.118.45.212	China	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.71	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/matehamatpash/pages/dover.aspx	Block	1
182.118.55.118	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/926-he/refuah.aspx	Block	1
62.210.88.201	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
84.94.161.105	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1148-he/chinuch.aspx	Block	1
40.77.167.57	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
182.118.60.35	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.65.17	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71866-he/maarachot.aspx	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
40.77.167.68	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	1
212.49.107.118	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
182.118.60.35	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1