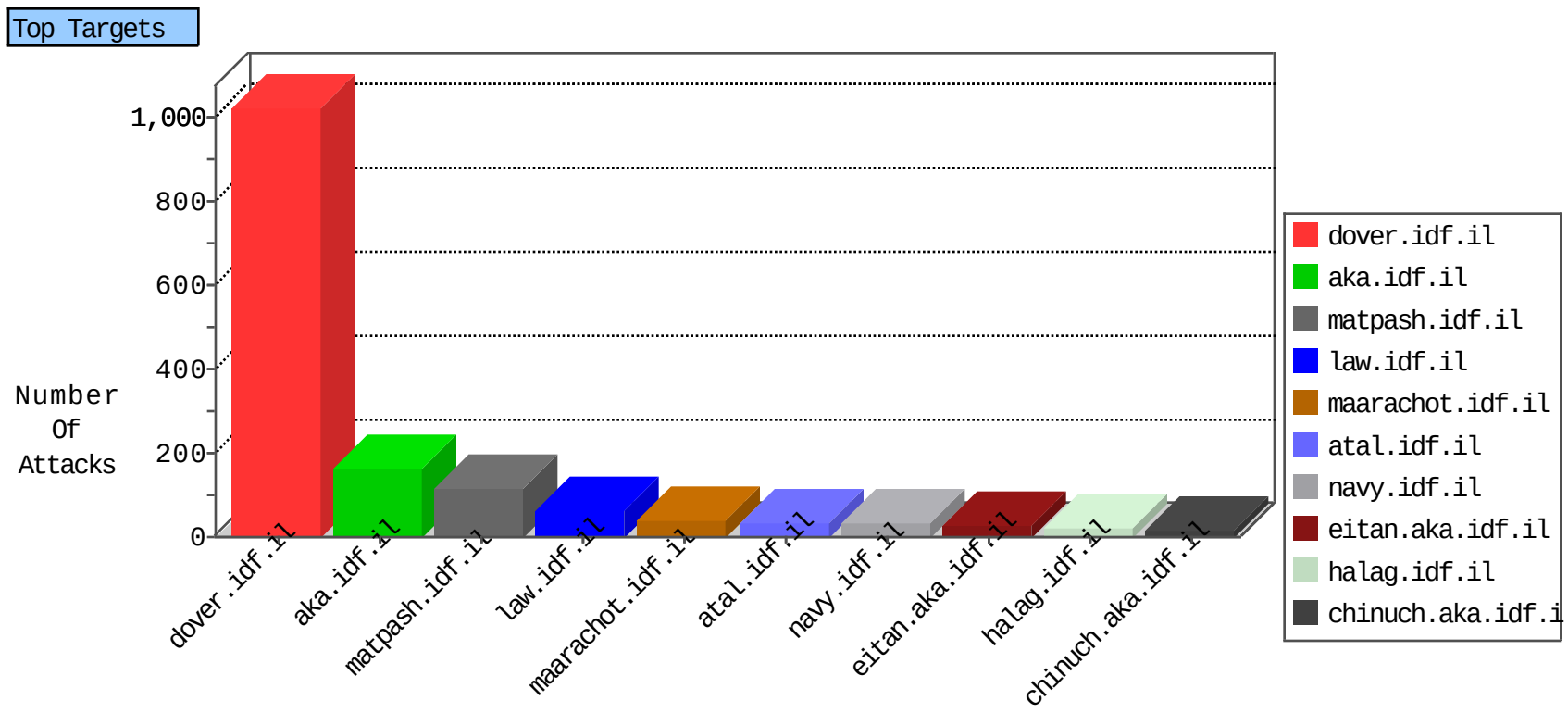
10-31-2015-06:04:04 to 10-31-2015-07:04:04

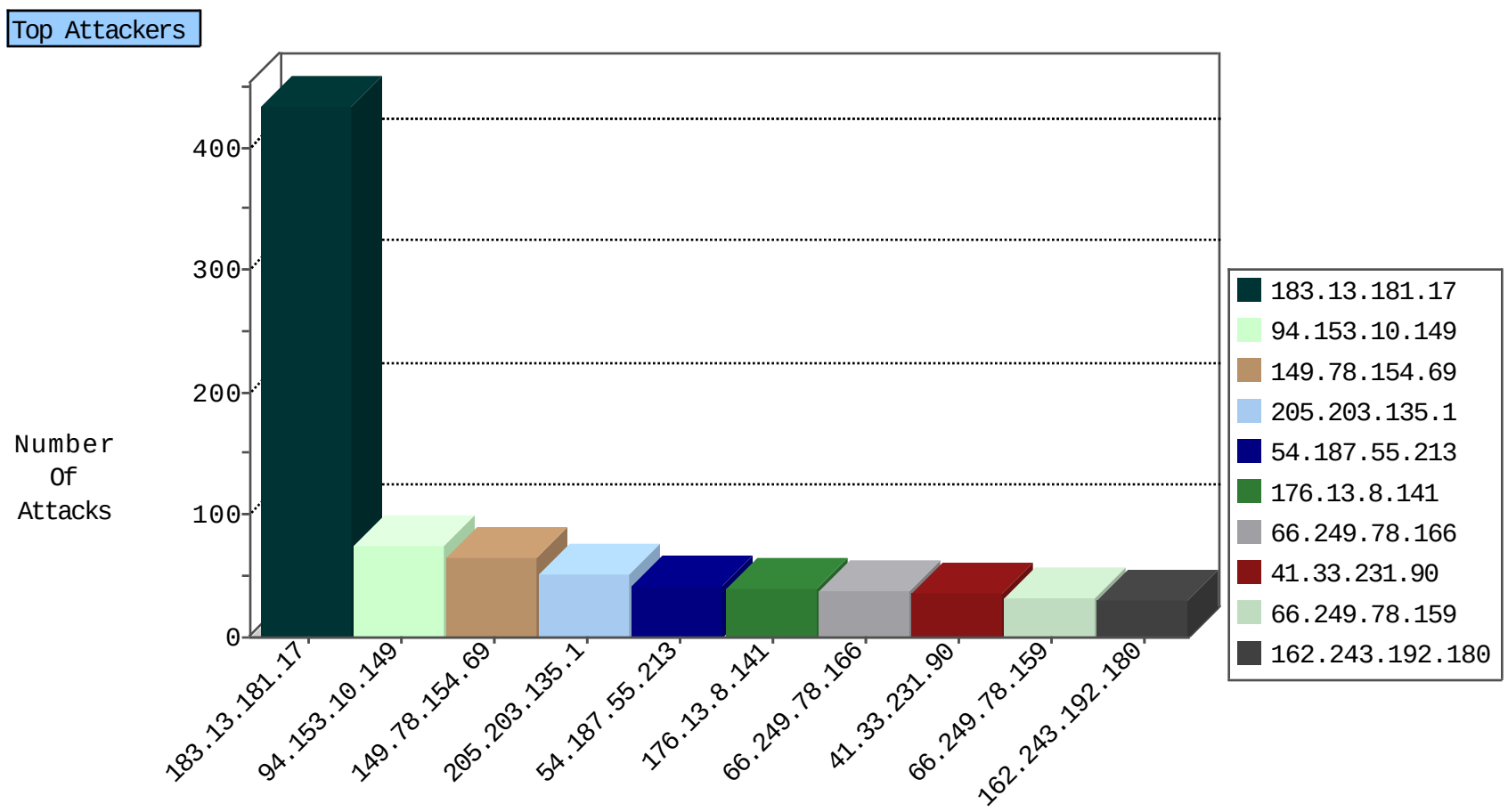
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-31-2015-06:04:04 to 10-31-2015-07:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7150
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
185.5.222.138	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.39	mobile.meitav.idf.i	JLM_Under_Attack_Con_Http	drop	2
112.175.228.17	Korea, Republic of	147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	1
142.4.105.172	United States	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Http	drop	1
112.175.228.17	Korea, Republic of	147.237.76.39	mobile.meitav.idf.i	Invalid TCP Flags	drop	1
142.4.105.172	United States	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Http	drop	1
112.175.228.17	Korea, Republic of	147.237.76.197	e.himush.idf.il	Invalid TCP Flags	drop	1

10-31-2015-06:04:04 to 10-31-2015-07:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-31-2015-06:04:04 to 10-31-2015-07:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-31-2015-06:04:04 to 10-31-2015-07:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.13.8.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.1.104		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
70.27.111.214	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
108.75.133.30	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.166.22.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
14.201.169.193	Australia	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
172.0.118.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	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
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.125.75.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.100.61.170		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
200.104.52.36	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
69.171.231.225	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
219.75.100.65	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
75.137.113.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
69.171.231.224	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
45.50.179.51		147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.136.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.114.251.33	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.6	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.176.208.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.58.103.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.69.220.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.165.15.79	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.138.237.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
125.202.25.184	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
38.111.147.88	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.13.181.17	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.13.181.17	Block	360
183.13.181.17	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	75
94.153.10.149	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 94.153.10.149	Block	45
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	30
162.243.192.180	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/14-he	Block	15
79.182.109.25	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	15
66.249.69.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
151.80.31.127	Italy	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
162.243.192.180	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	15
79.182.109.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1446-he/atal.aspx	Block	15
66.249.67.91	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/1090-he/halag.aspx-publisher=	Block	15
157.55.39.10	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	15
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71936-he/maarachot.aspx	Block	15
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	15
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	15
66.249.74.96	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/silvanshalom.aspx	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	15
157.55.39.50	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	15
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	15
176.13.1.11	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	15
94.153.10.149	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	15
66.249.75.70	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74/	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/main/rabanut/general.aspx	None	15
157.55.39.160	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	15
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1317-he/atal.aspx	Block	15
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17899-he/kkkkkkk=70d4317dkkkkkkk_70d4317d	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
94.153.10.149	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	15
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	15