

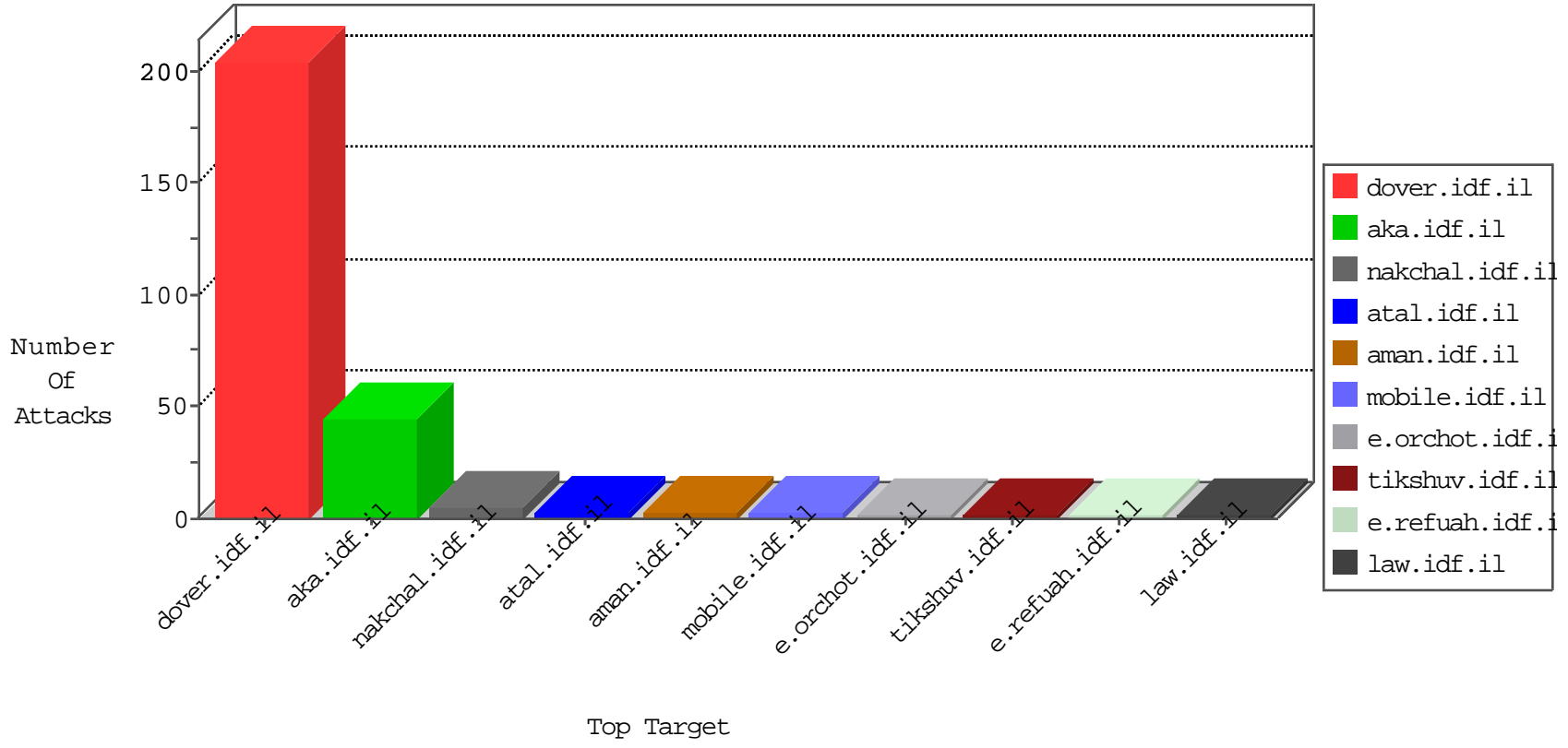


# IDF Under Attack

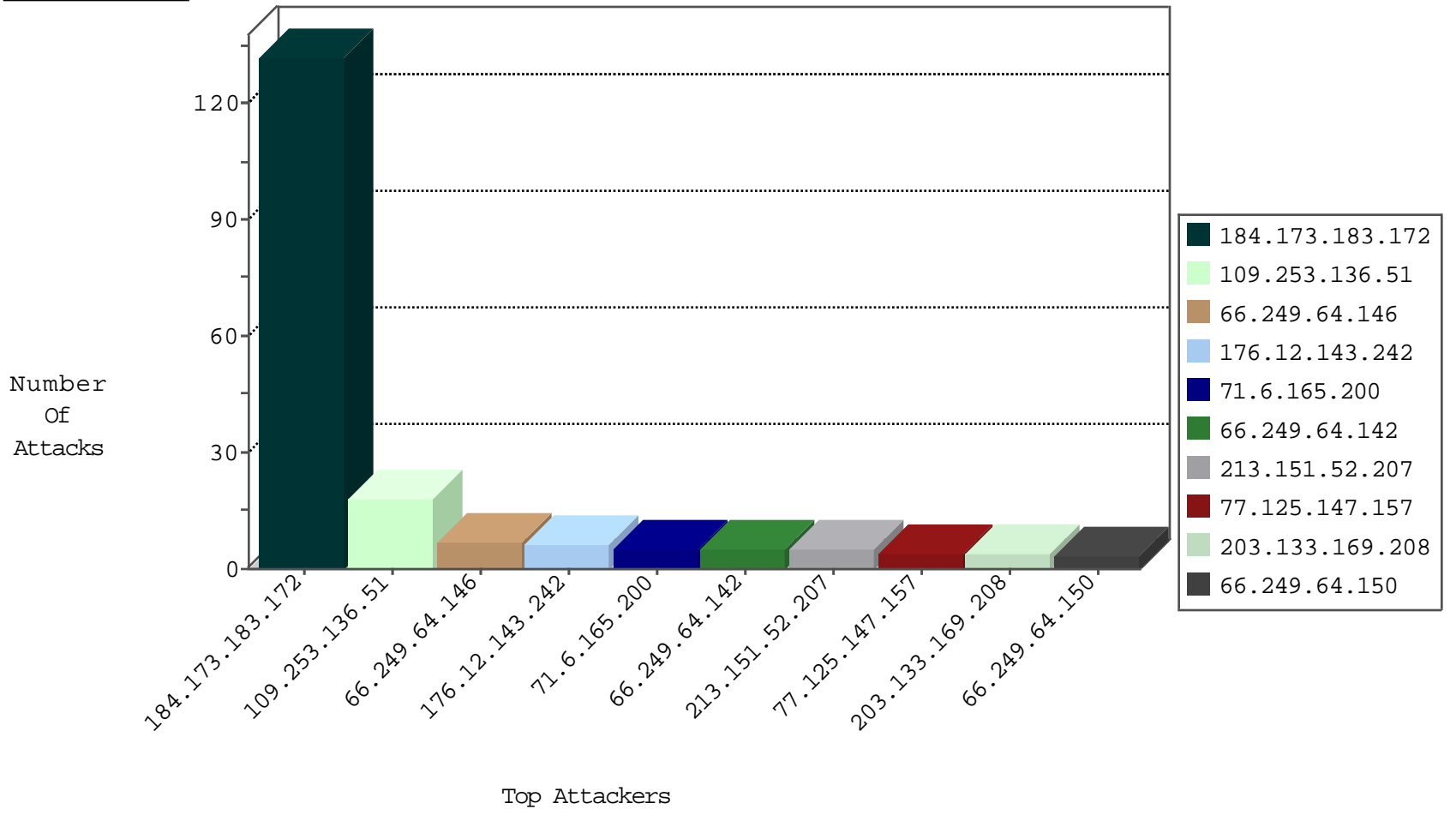
03-31-2015-17:03:01



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
62.219.0.106	Israel	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
62.219.0.106	Israel	147.237.76.198	e.yohanan.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	132
104.175.206.11		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.31.57.5	Italy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	2
77.109.141.138	Switzerland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
84.109.209.33	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.125.147.157	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.97.160	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
37.187.244.40	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
212.235.67.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
78.46.66.41	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
176.10.99.207	Switzerland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.235	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.115.94.243	Anonymous Proxy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
84.109.86.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.65.68.58	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
93.173.57.42	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
------------------	------------------	----------------	------	------	-------

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.136.51	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.143.242	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
37.26.147.235	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
62.219.24.52	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
119.191.1.105	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.64.146	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.146	Block	7
213.151.52.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.208	Block	4
66.249.64.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/izkor/print_bottom.asp	Block	4
46.19.86.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
77.127.221.45	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
80.246.133.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/izkor/print_bottom.asp	Block	2
77.125.147.157	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
109.253.137.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.95	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.224.72.203	Germany	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Parameter Value at 1 for www.idf.il/templates/social/i% <i>i</i> %v	Block	1
66.249.69.20	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.143.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/forgotpassword.aspx	None	1
109.254.67.32	Ukraine	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
85.65.2.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.13.50	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
193.43.244.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
66.249.64.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.142	Block	1
2.52.47.94	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.64.14.144	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.69.28	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
176.12.148.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
113.92.249.217	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
85.65.229.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
217.132.94.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	1
195.144.71.107	Belgium	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
157.55.39.215	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
31.13.112.122	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/901-8271-he	Block	1
109.160.141.132	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache httpd Remote Denial of Service ME	Block	1
212.147.17.58	Switzerland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.147.17.58	Block	1
84.108.43.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	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
176.12.148.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
123.192.136.97	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.116.204.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.48.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.178.211.89	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
164.138.113.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
31.168.77.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...36&docid=74856	Block	1
109.253.132.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.147.17.58	Switzerland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/errors/errtimeout.asp	Block	1
84.111.103.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
178.219.249.134	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.42	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
49.214.41.205	Taiwan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
93.173.53.247	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1