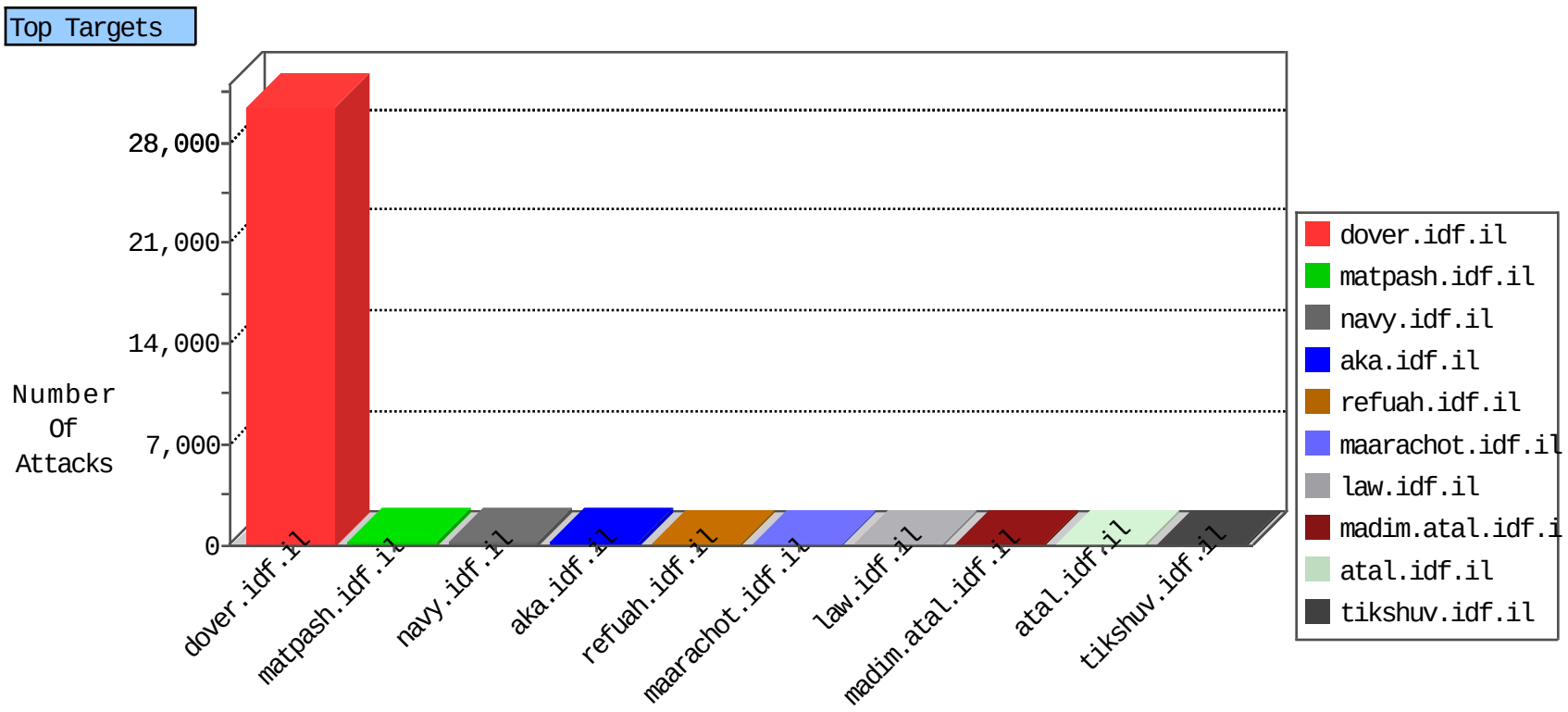
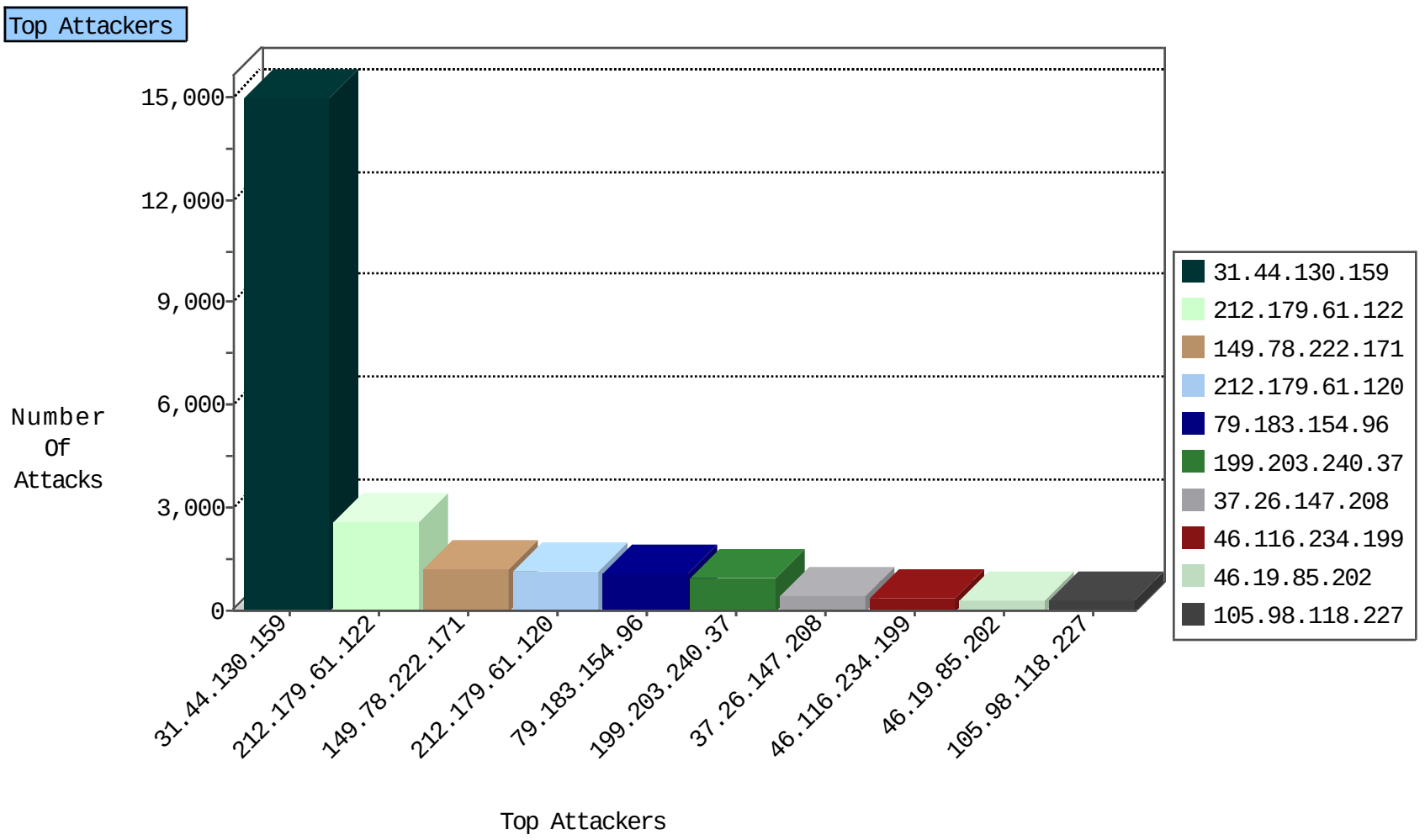
04-09-2015-13:03:03 to 04-09-2015-14:03:03

IDF Under Attack
04-09-2015-13:03:03

Top Targets



Top Attackers



04-09-2015-13:03:03 to 04-09-2015-14:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
41.234.12.26	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	258
93.173.28.75	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	228
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	101
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	96
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	92
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	88
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	80
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	77
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	70
80.246.136.222	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	66
66.249.93.158	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	65
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	65
105.98.118.227	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
66.249.93.154	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	44
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	32
66.249.93.162	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	31
66.249.93.186	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	30
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	28
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	26
66.249.93.190	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	23
66.249.89.95	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.89.91	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	19
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	19
66.249.93.194	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	18
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	15
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.73.239	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	13
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	11
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
162.243.147.149	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.78.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.89.95	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.83	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.73.231	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	7
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
66.249.78.113	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.78.167	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6

04-09-2015-13:03:03 to 04-09-2015-14:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.176.183.73	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.19.85.89	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.0	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.108.116.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
2.54.25.203	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
79.177.166.155	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.65.162.193	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.43	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.178.164.253	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
46.19.85.63	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-09-2015-13:03:03 to 04-09-2015-14:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
149.88.142.206	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.117.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.210.186.156	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

04-09-2015-13:03:03 to 04-09-2015-14:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
31.44.130.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15017
212.179.61.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2601
149.78.222.171	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1192
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1179
79.183.154.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1101
199.203.240.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	979
37.26.147.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	403
46.116.234.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	353
46.19.85.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	306
5.29.158.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	293
89.139.174.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	275
65.49.68.199	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
2.54.28.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	151
87.69.154.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	123
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
46.19.86.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	81
105.98.118.227	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
149.78.125.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
46.19.85.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
213.57.41.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
2.54.146.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
2.54.148.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
79.177.185.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
77.127.106.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
78.95.93.133	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
192.131.85.210	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
176.12.140.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
46.121.26.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
176.12.144.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
109.253.149.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
176.12.139.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
176.12.143.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.144.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.159.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
46.116.203.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
109.253.136.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
84.108.30.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
37.26.147.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
46.19.86.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
95.186.95.205	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
84.108.152.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
176.12.146.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
176.12.151.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.136.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
46.19.85.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
37.26.147.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
176.12.138.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
41.234.12.26	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
105.98.118.227	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.118.227	Block	98
105.98.118.227	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	94
79.178.119.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	10
85.250.186.155	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	6
41.131.117.128	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	4
2.54.128.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
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	2
105.98.118.227	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	2
84.111.37.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
50.84.247.238	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
37.59.55.128	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper	Block	1
149.78.166.54	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.115.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
79.177.112.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8903-he/refuah.aspx	Block	1
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.65.73.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.1.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
50.84.247.238	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
37.142.135.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
149.88.12.219	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.110	France	147.237.76.30	himush.idf.il	Unknown Parameter SortDir in www.chimush.atal.idf.il/1324-he/himush.aspx	None	1
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=552653faf55fd928000; __atssc=facebook%3B3	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.66.154.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.228.94.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
167.114.118.4	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//templates/shared/usercontrols/promotioncube/	Block	1
80.246.130.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.117.240.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
37.59.55.128	France	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	1
132.72.100.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
77.125.214.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
176.12.136.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
84.108.71.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
46.121.99.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
37.59.55.128	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 37.59.55.128	Block	1
149.78.13.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.210.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
79.176.183.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
176.12.140.209	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.64.57.60	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1