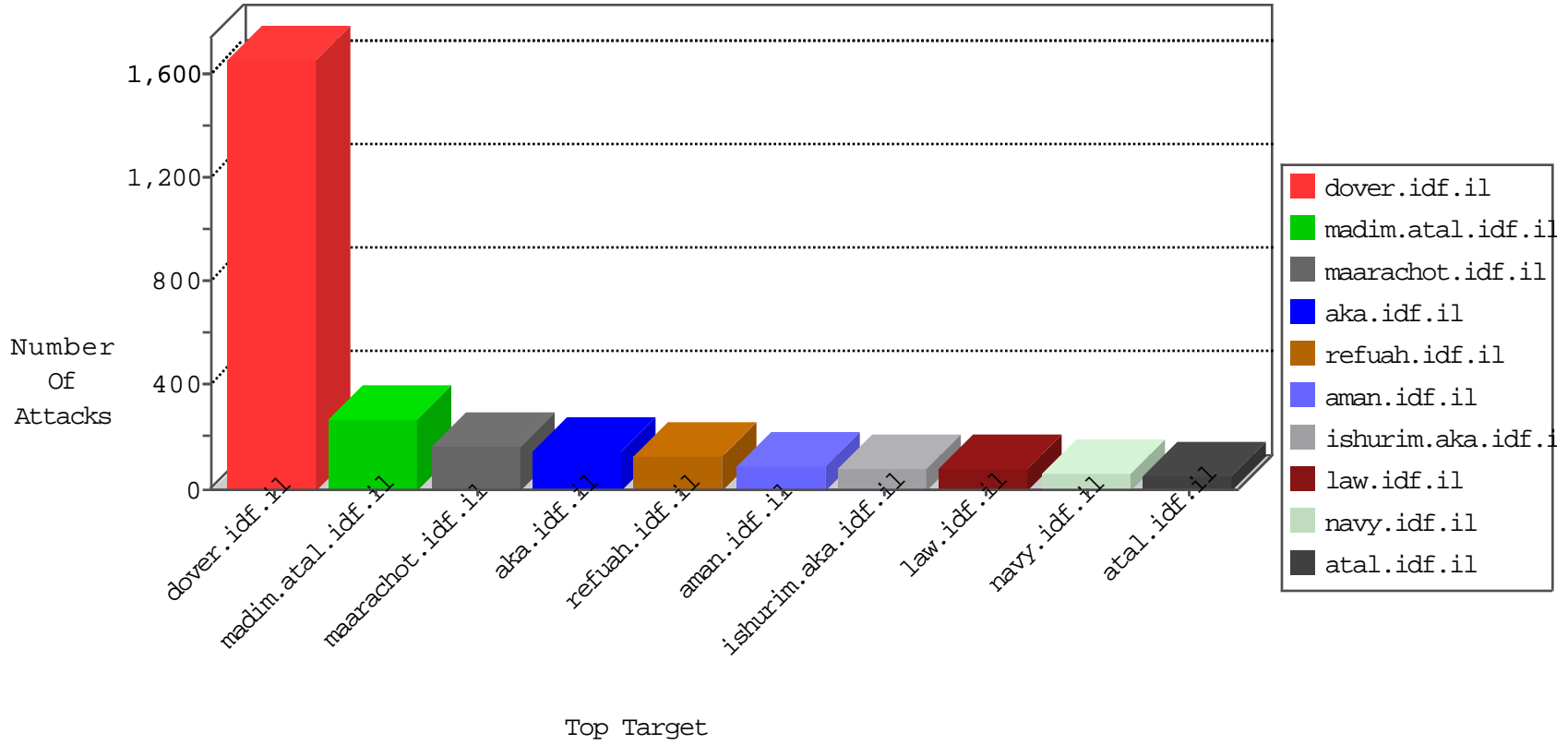
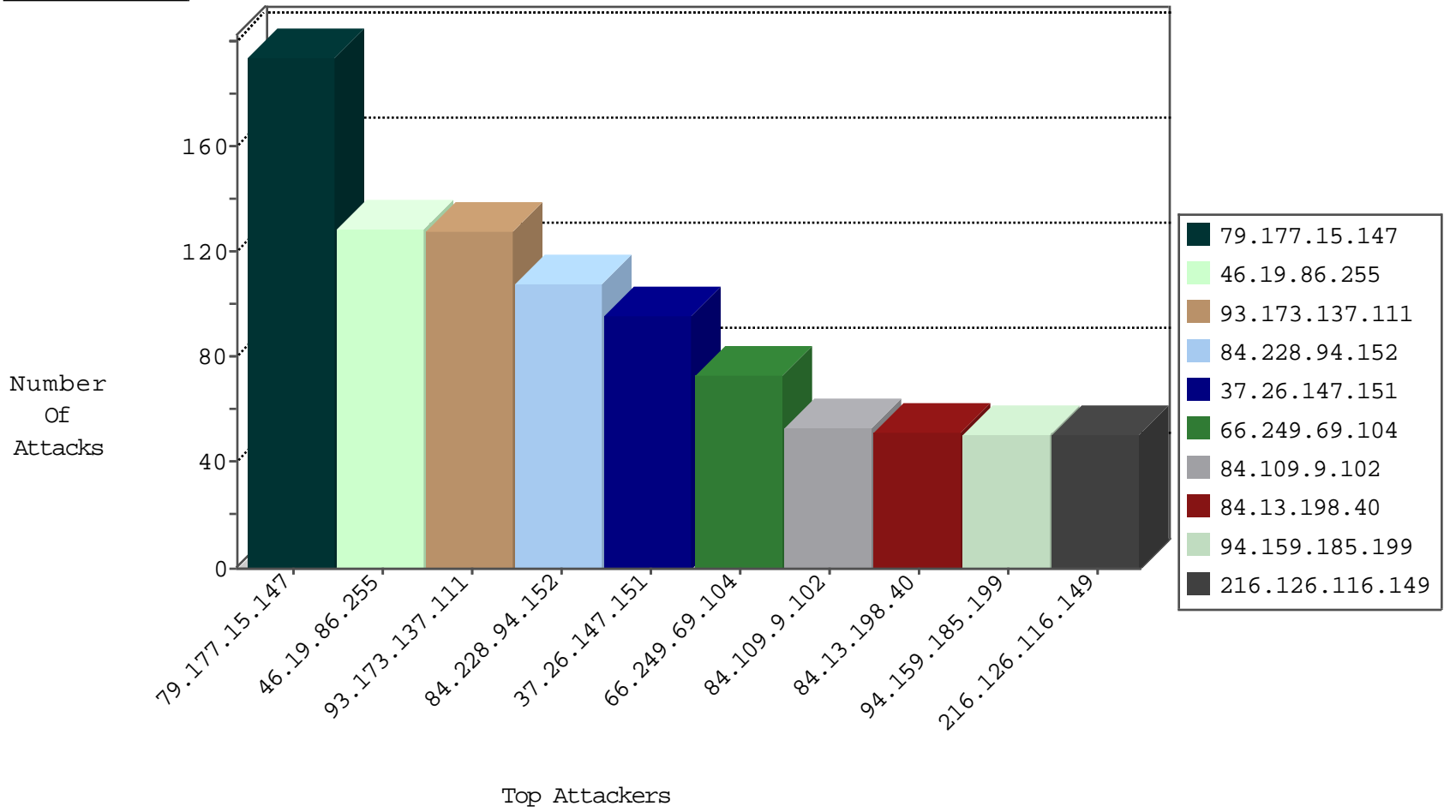




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.83	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	4427
109.66.129.224	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	599
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
46.116.233.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
85.64.125.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
79.182.182.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
66.249.69.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	73
66.249.69.96	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	49
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	42
66.249.69.88	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	40
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	31
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	28
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	24
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
79.181.109.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	19
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	18
46.19.86.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	16
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.64.96	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	13
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	13
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	12
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
82.80.155.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.69.39	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.81.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.69.31	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.64.87	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
85.250.135.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
80.246.136.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
93.120.27.62	Romania	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.172.105.45	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
212.179.5.3	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.250.135.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
84.110.60.143	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	2
2.54.188.139	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.42.11	China	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.117.208.243		147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.7.37.194	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
80.246.141.54	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.7.37.194	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
218.7.37.194	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
149.78.26.166	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.212.89	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.136.228	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
99.59.38.233	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.91.58	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.51.140	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.114.97	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.7.37.194	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
218.7.37.194	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
79.177.178.166	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.7.37.194	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.2	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
113.21.226.56	New Zealand	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.9	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.23.106	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.151	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.135.85	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.177.15.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	194
84.228.94.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	108
37.26.147.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
84.13.198.40	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
94.159.185.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
216.126.116.149	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
84.109.9.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
79.178.105.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
79.181.179.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.253.136.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
109.253.136.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
84.111.210.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
24.142.153.50	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
93.172.105.45	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	26
109.253.142.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
79.182.195.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
79.178.118.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
46.19.86.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
212.179.61.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
192.116.131.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.86.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
82.145.219.177	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
67.200.239.195	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
2.54.41.189	Israel	147.237.72.167	ishurim.aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	11
109.253.129.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
192.116.108.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
80.230.79.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
2.54.152.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
85.64.154.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
77.127.151.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.172.138.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.29.245.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
109.64.125.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
37.142.226.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
80.179.223.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
67.194.229.137	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.108.234.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
149.78.58.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.117.163.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	129
93.173.137.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
2.54.62.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
213.57.252.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	4
109.66.168.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.187.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.148.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
84.109.9.102	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.109.9.102	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
109.160.217.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
164.138.125.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
85.250.190.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.38.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.150.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.178.202.64	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.120.148.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.26.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.89.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
31.13.112.117	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files	Block	1
164.138.124.27	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
37.142.125.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
87.69.194.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
2.54.37.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.2.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.97.252	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/https://www.idf.il/	Block	1
54.159.92.113	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
31.13.112.122	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/2	Block	1
95.86.89.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$cphSachar\$txtMisparIshi in aka.idf.il/main/sachar/	None	1
84.109.9.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/6_s3_	Block	1
74.220.219.74	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
164.138.125.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.105.45	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
79.181.184.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
149.88.58.73	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/	None	1
62.0.200.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.44.134.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
96.42.181.72	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
84.111.37.182	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
74.220.219.74	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
109.253.133.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.203.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/homas/site/homasformphase4.aspx	None	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
69.16.243.169	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
31.44.143.75	Israel	147.237.72.166	aka.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
96.42.181.72	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
109.253.158.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.116.148.27	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
95.86.89.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1