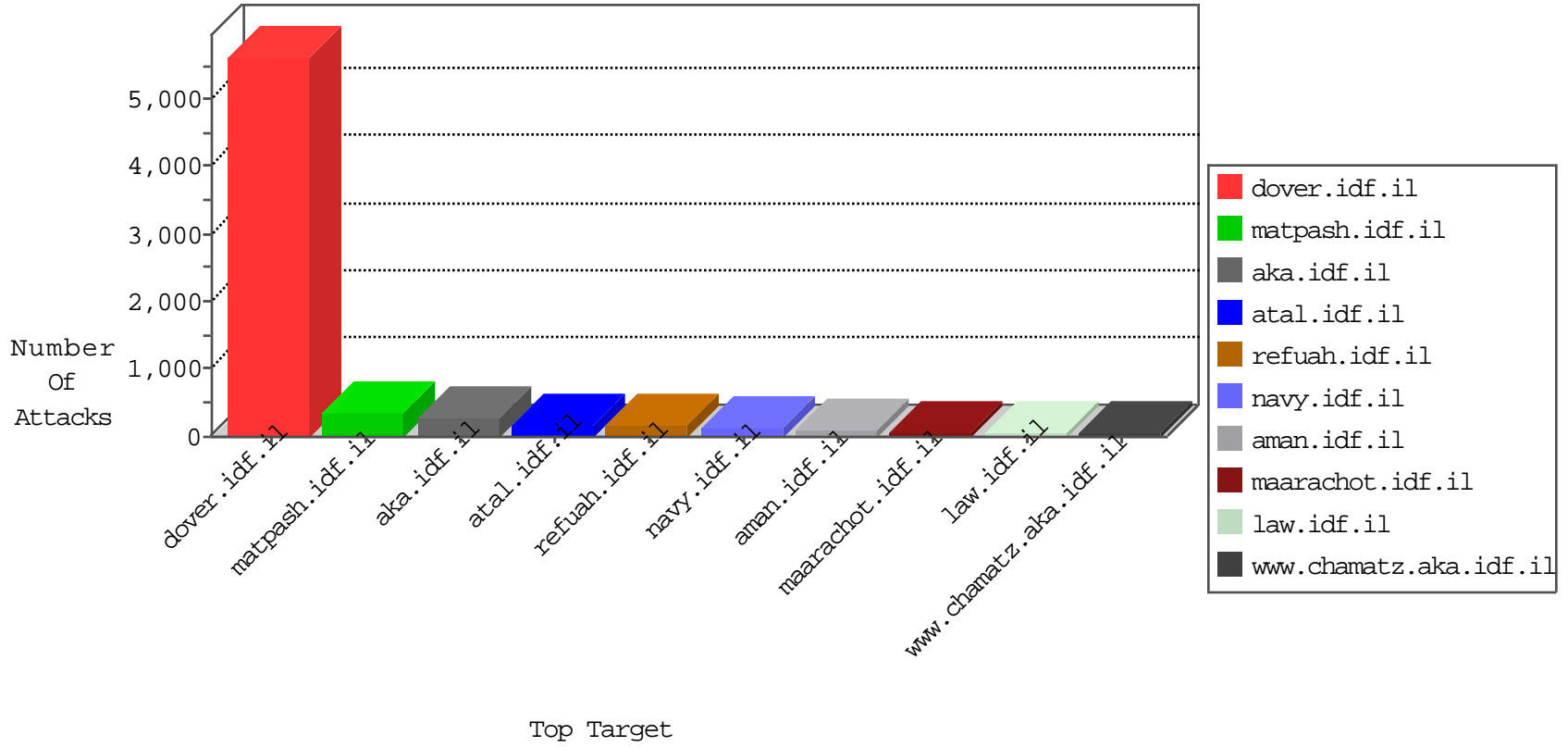
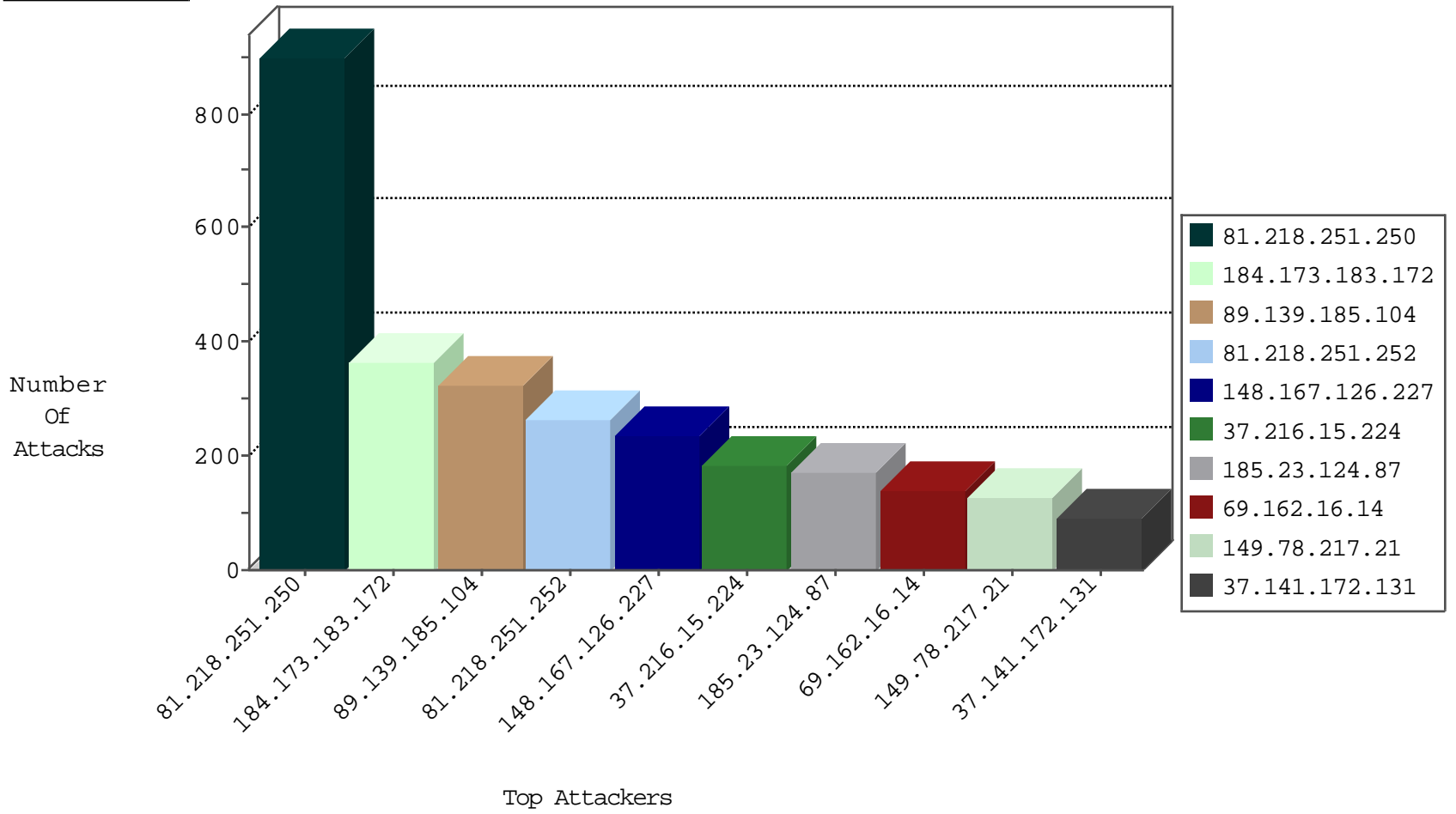




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
217.132.84.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	351
84.228.138.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
84.228.139.247	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
85.65.2.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
109.67.0.39	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
212.76.119.201	Israel	147.237.77.216	doover.idf.il	SYN Flood unverified cookie	drop	67
66.249.93.168	United States	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	52
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	46
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	44
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	38
66.249.93.160	United States	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	36
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	24
66.249.93.162	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	24
66.249.93.164	United States	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	22
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	22
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	21
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.64.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.64.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	18
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	16
66.249.78.159	United States	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	16
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.64.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	15
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.166	United States	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	14
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.93.158	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.93.154	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.11	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.93.240	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.80.75	United States	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	9
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	231
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	131
64.79.144.10	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	57
79.181.35.121	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
209.253.226.1	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.179.20.214	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
105.210.58.201	South Africa	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.245	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.109.85.105	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.64.132.111	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
2.54.163.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.177.150.19	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	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
46.19.85.32	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.64	Israel	147.237.76.31	nakchal.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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
37.142.248.145	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.101.21.179	Russian Federation	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.101.21.179	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.101.21.179	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.118	Switzerland	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
140.119.80.110	Taiwan	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
82.117.208.243		147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
54.69.194.190	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.101.21.179	Russian Federation	147.237.76.198	e.yochalan.idf.il	ET SCAN Potential SSH Scan	1
46.101.21.179	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
41.130.43.244	Egypt	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
169.54.233.118	Switzerland	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
140.119.80.110	Taiwan	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	898
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	323
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	263
148.167.126.227	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	234
37.216.15.224	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	185
185.23.124.87	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	172
69.162.16.14	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	138
149.78.217.21	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	125
37.141.172.131	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
37.26.146.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
178.11.176.10	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	85
5.108.0.126	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
109.253.142.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
45.101.65.52		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
109.110.118.146	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
197.133.127.214	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
37.26.147.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
137.135.176.175	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
82.114.168.158	Yemen	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
197.203.139.237	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
46.116.180.171	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	45
85.65.64.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
176.67.99.176	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
86.91.178.232	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
178.240.215.39	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
46.19.85.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
77.127.87.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
167.220.149.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
109.253.147.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
188.55.64.178	Saudi Arabia	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	29
46.19.85.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
105.210.58.201	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
41.130.43.244	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
137.135.176.175	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
197.134.127.211	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.136.235.137	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
109.253.157.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
82.145.217.195	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
85.65.170.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
93.173.63.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
92.241.42.72	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
83.185.83.159	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.138.240.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
167.114.64.100	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	3
207.46.13.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
31.210.189.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
37.26.147.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.115.187.54	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
128.237.214.154	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.0.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
79.182.132.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	1
41.239.34.248	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
149.88.30.244	United States	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
85.64.214.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
71.245.113.228	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.157.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.5.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationsservice.aspx/getuserdetails	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/december/30a.stm	Block	1
46.19.86.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.7.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationsservice.aspx/getuserdetails	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.139.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.253.157.138	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
80.230.124.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
50.87.15.225	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.180.21.109	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
209.203.10.195	South Africa	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
188.143.232.21	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.59.29.19	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
112.111.188.90	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
194.243.81.177	Italy	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
50.87.15.225	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.233	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1122-he/nakchal.aspx	Block	1
93.173.145.127	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.154.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
209.203.10.195	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8750-he/refuah.aspx	Block	1
194.243.81.177	Italy	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.54.153.178	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
160.79.139.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.66.187.12	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1