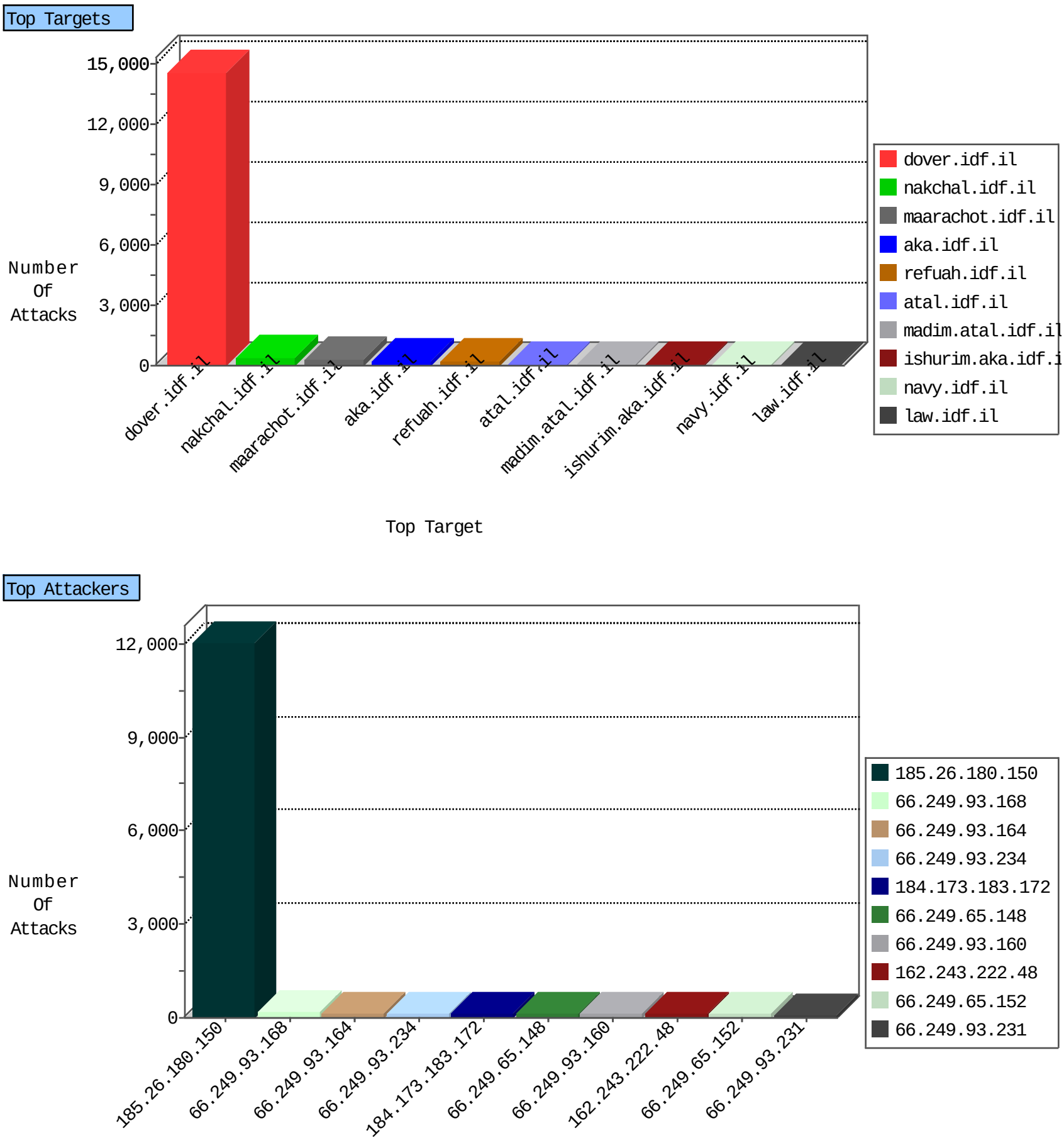
04-12-2015-23:03:07 to 04-13-2015-00:03:07

IDF Under Attack
04-12-2015-23:03:07



04-12-2015-23:03:07 to 04-13-2015-00:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.172	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3402
149.78.138.255	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	348
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	151
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	143
66.249.93.234	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	130
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	124
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	117
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	108
66.249.93.231	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	105
66.249.93.237	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	101
185.26.180.150	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	80
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	67
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	43
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	37
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	35
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	32
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	18
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.93.168	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	11
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.21	United States	147.237.76.42	refuah.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	10
66.249.73.140	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	8
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.64.88	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	8
66.249.64.92	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	8
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.65.191	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.64.87	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.93.172	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.73.132	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
212.76.101.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5

04-12-2015-23:03:07 to 04-13-2015-00:03:07

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	127
46.19.85.144	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
108.58.15.82	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.228.110.197	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
50.44.57.104	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.82.70.198	Netherlands	147.237.77.178	e.matpash.idf.il	DVRep_P-N_40-59	Permit	1
46.19.85.80	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.76.44	e.refuah.idf.il	DVRep_P-N_40-59	Permit	1
84.109.216.123	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.76.196	e.sviva.idf.il	DVRep_P-N_40-59	Permit	1
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
80.82.70.198	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.76.198	e.yohalan.idf.il	DVRep_P-N_40-59	Permit	1
93.120.27.62	Romania	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
80.82.70.198	Netherlands	147.237.8.27	e.madim.atal.idf.il	DVRep_P-N_40-59	Permit	1

04-12-2015-23:03:07 to 04-13-2015-00:03:07

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	7
84.229.183.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
125.5.16.195	Philippines	147.237.77.243	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.5.16.195	Philippines	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.238.134.92	Poland	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
196.47.173.21	Cote D'Ivoire	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
196.47.173.21	Cote D'Ivoire	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
176.12.138.5	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
125.5.16.195	Philippines	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.67.114	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	1
79.176.0.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.136.84.245	Germany	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

04-12-2015-23:03:07 to 04-13-2015-00:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.150	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12038
162.243.222.48	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	115
79.176.114.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	92
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
137.122.64.42	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
46.19.85.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	75
80.12.39.223	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
50.44.57.104	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
67.85.181.13	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
168.63.137.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
85.250.135.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
46.19.85.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
109.253.144.98	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.144.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
87.69.178.80	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
66.102.88.107	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
71.205.114.88	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
84.228.27.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
176.12.142.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
77.127.110.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
207.46.13.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
93.172.144.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
192.114.91.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.253.128.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
80.215.178.109	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
109.253.137.243	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
79.182.15.67	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
5.29.100.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
17.142.152.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
79.183.99.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
85.64.214.10	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	11
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
17.142.152.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
17.142.152.110	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
17.142.145.3	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
84.229.183.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.253.144.80	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.253.135.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
17.142.152.81	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
77.125.127.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
79.52.47.119	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
207.46.13.82	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
98.210.231.138	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
87.68.61.222	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
79.181.140.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
87.69.213.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/panmaz/index.stm	Block	3
176.10.104.234	Switzerland	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 176.10.104.234	Block	3
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
109.64.57.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
77.127.170.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
196.22.134.131	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
37.187.146.46	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.22.217.111	Germany	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 91.22.217.111	Block	2
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
176.10.104.234	Switzerland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/900-en/	Block	1
37.57.208.151	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/skira/default.asp	None	1
109.66.133.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
212.74.197.3	Russian Federation	147.237.72.166	aka.idf.il	Unknown HTTP Request Method COOK in URL www.aka.idf.il/brothers/skira/default.asp	Block	1
185.32.179.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$LoginControl$captcha$captchaText in www.aka.idf.il/main/giyus/default.aspx	None	1
79.178.3.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.28.181.122	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
196.22.134.131	South Africa	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
84.109.209.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.141.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.186.15.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.187.146.46	France	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
87.68.74.35	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
212.199.218.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
188.135.40.206	Oman	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/80	Block	1
79.180.110.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/personalentrance.asp	Block	1
46.120.55.8	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.102.254.46	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
109.64.187.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
84.111.240.29	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/901-7739-he/tikshuv.aspx	Block	1
77.127.170.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
176.12.145.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.222.178	United States	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
157.55.39.172	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
46.216.168.21	Belarus	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/skira/default.asp	None	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	1
109.65.1.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl05 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.228.50.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTARGUMENT in www.aka.idf.il/main/sachar/	None	1
79.176.152.78	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
176.67.84.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
151.249.186.121	Czech Republic	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/printpreview/default.asp	None	1
37.238.144.8	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atr/	Block	1
80.246.130.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1