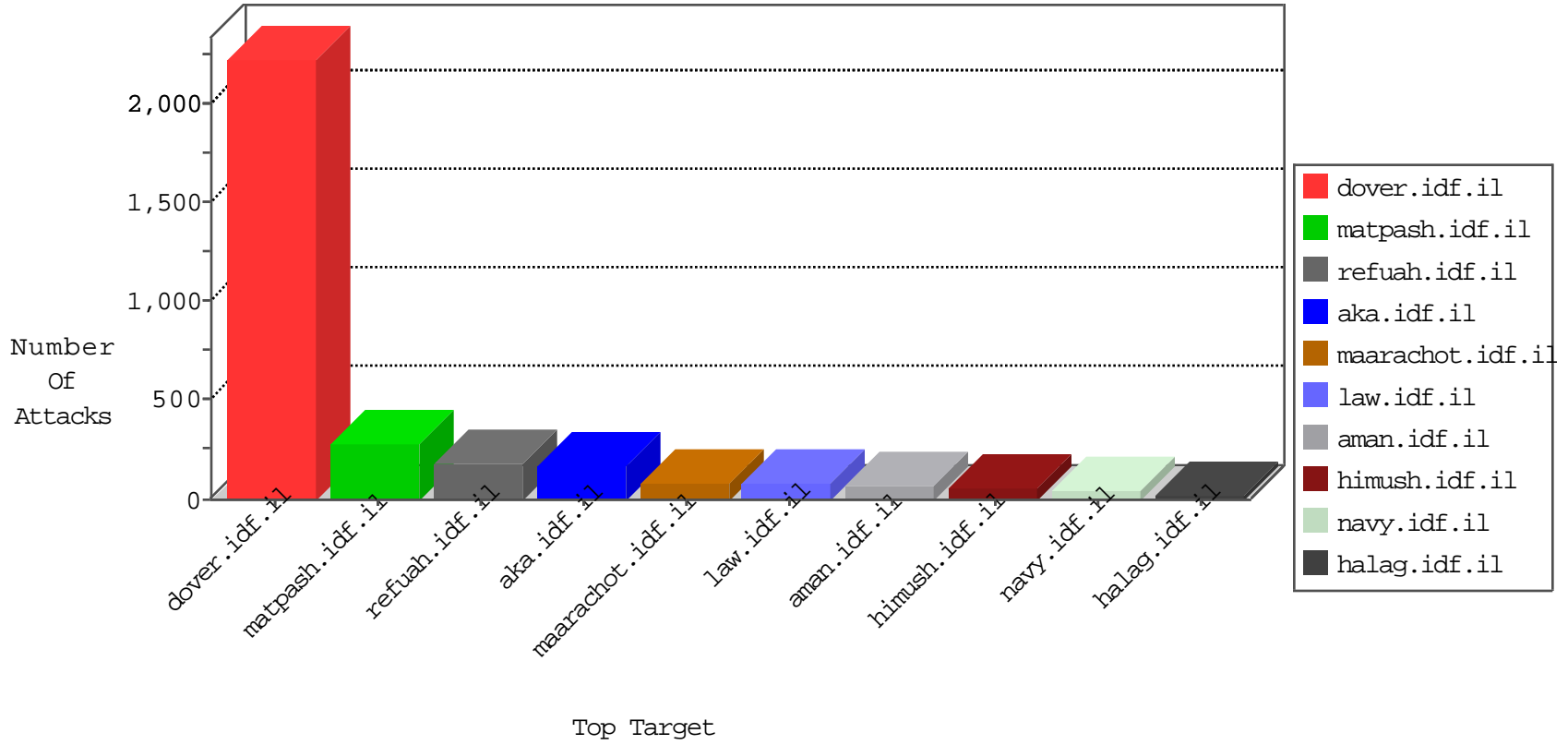
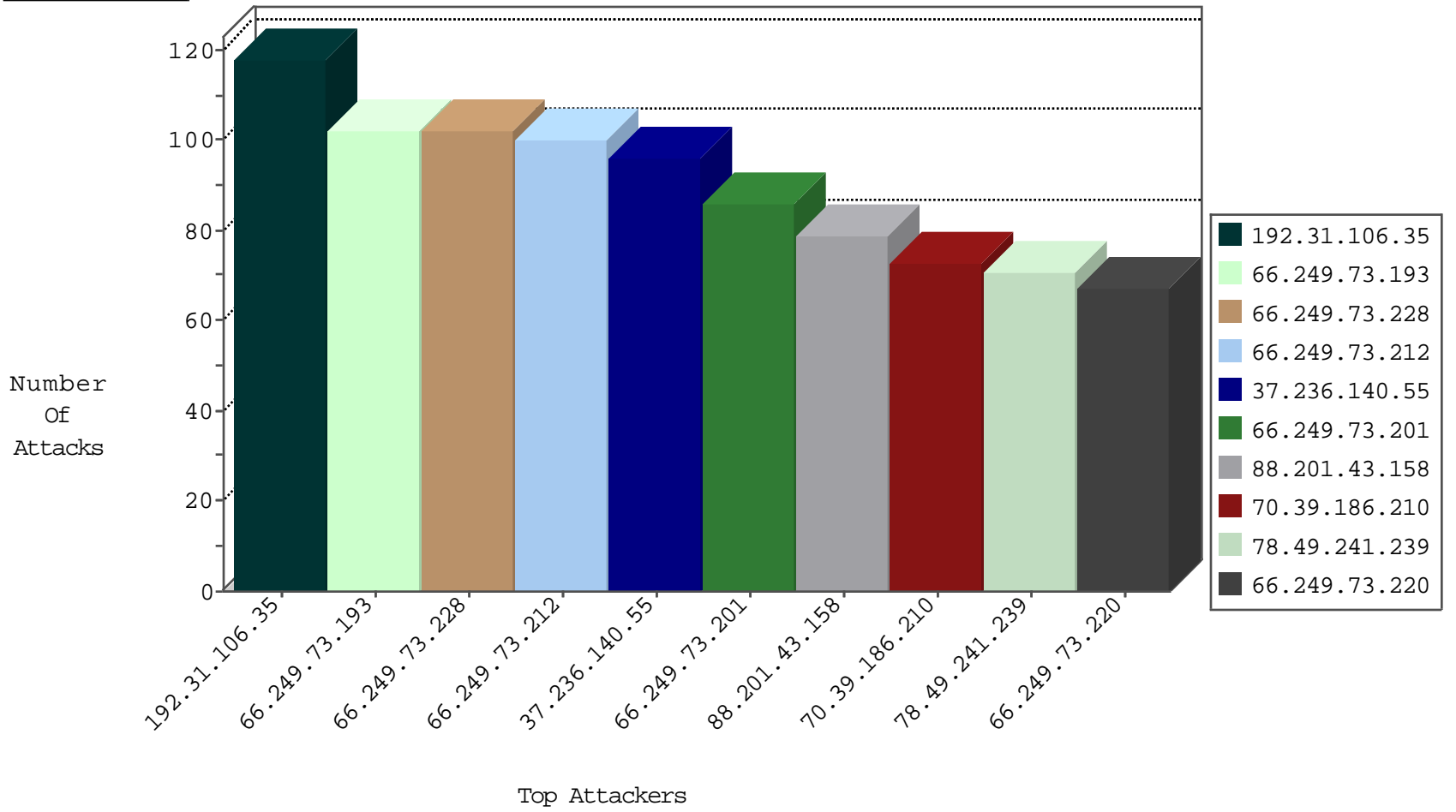




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.146	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3769
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	393
5.29.201.236	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	392
109.65.65.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	102
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	102
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	100
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	86
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	67
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	52
66.249.67.107	United States	147.237.76.30	himush.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	35
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	34
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	32
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	32
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	32
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	31
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
66.249.93.160	United States	147.237.77.216	dover.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
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
190.18.139.245	Argentina	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.73.223	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	12
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.65.188	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.73.231	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	8
66.249.93.162	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	7
93.172.46.62	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.67.30	United States	147.237.76.86	navy.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	6
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.75.111	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.93.171	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	6
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.65.181	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.65.192	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.81.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
73.16.142.112	United States	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
79.240.237.185	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.138.13.62	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
24.90.111.185	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.142.214.80	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	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	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	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
109.160.187.141	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 Ddos attack	2
93.172.46.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.64.180.14	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
69.12.92.160	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
162.253.66.50	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
123.57.81.67	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
123.57.81.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
123.57.81.67	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
110.173.177.37	India	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
110.173.177.37	India	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
81.200.91.2	Russian Federation	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
178.19.107.114	Poland	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
141.212.122.128	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
123.57.81.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
123.57.81.67	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
123.57.81.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
110.173.177.37	India	147.237.8.14	e.orchot.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
192.31.106.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	115
88.201.43.158	Bahrain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	79
37.236.140.55	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
78.49.241.239	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
70.39.186.210	Satellite Provid	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
70.39.186.212	Satellite Provid	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
188.117.97.52	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
46.19.86.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
46.19.85.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
79.240.237.185	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.134.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
95.187.104.197	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.65.168.210	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
5.108.141.100	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
79.181.140.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.117.152.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
157.55.80.246	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
109.160.144.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
79.183.2.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
37.141.172.131	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
187.138.18.119	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
194.90.117.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
41.42.242.114	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
149.88.136.232	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
93.184.20.241	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
188.71.230.100	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.253.149.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.149.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
93.172.46.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.80.246	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.86.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
172.19.79.11		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
80.113.6.163	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
197.254.224.221	Sudan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
85.64.240.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
93.168.236.138	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.145.180	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
79.183.186.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.147.98	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
5.29.164.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
178.135.118.26	Lebanon	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
37.26.146.203	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
77.125.18.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.197.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigato n.asp	Block	12
79.177.27.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
77.125.158.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigato n.asp	Block	3
37.8.0.32	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
185.32.177.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
37.142.117.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.67	United States	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
85.64.230.112	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2003/october/27.stm	Block	2
142.4.38.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fckeditor/editor	Block	1
37.26.147.201	Israel	147.237.76.31	nakhal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
85.250.57.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
24.212.29.16	Canada	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18219-he/dover	Block	1
79.178.119.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.120.134.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.138.13.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/1210-3.stm	Block	1
24.212.29.16	Canada	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
84.109.3.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.236.140.55	Iraq	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 37.236.140.55	Block	1
188.138.1.218	Germany	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
89.138.196.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
24.212.29.16	Canada	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
176.12.145.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.239	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.139.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.147.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.244.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/fagselecion.aspx	None	1
188.165.15.239	France	147.237.72.166	aka.idf.il	Unknown Parameter CatID in www.aka.idf.il/giyus/atuda/	None	1