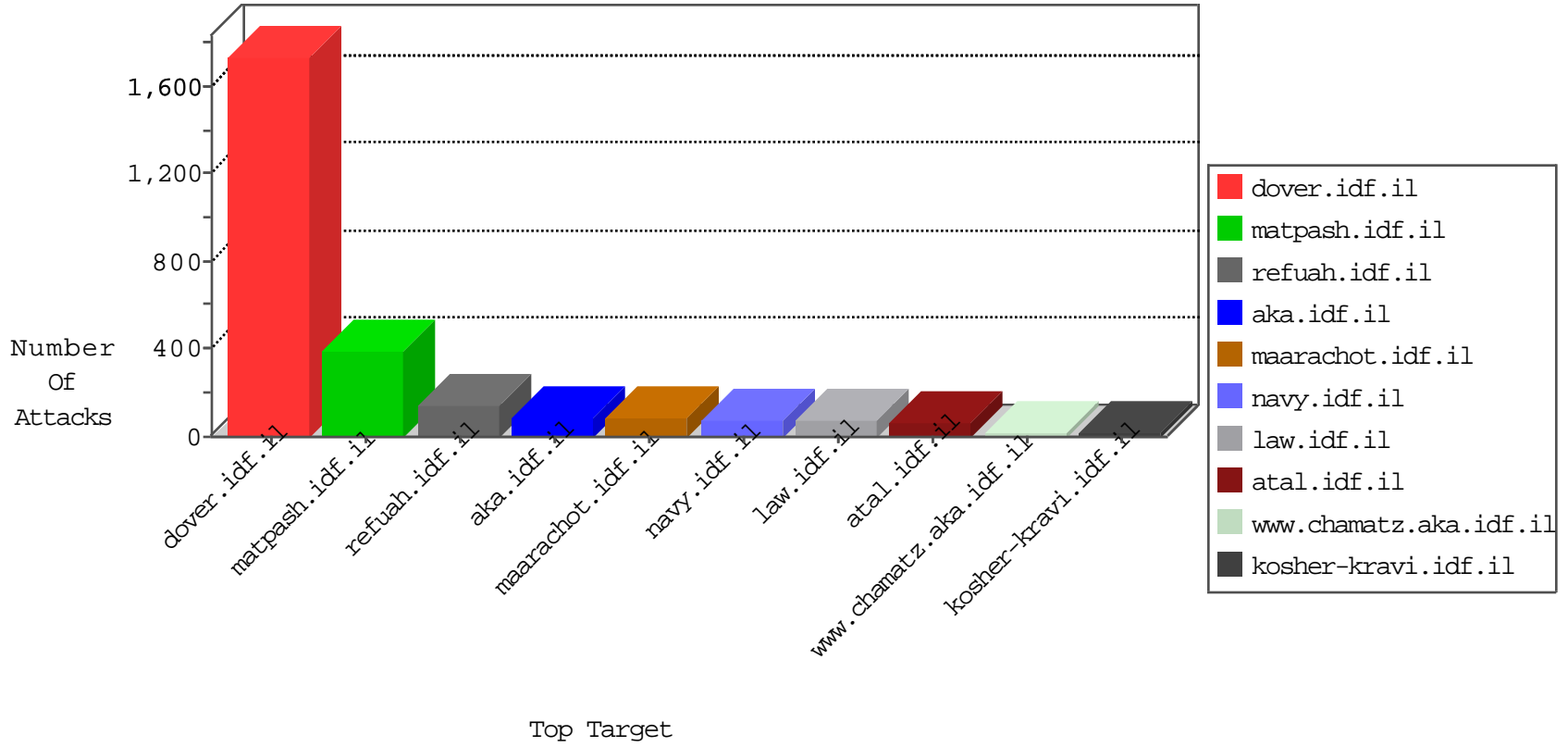
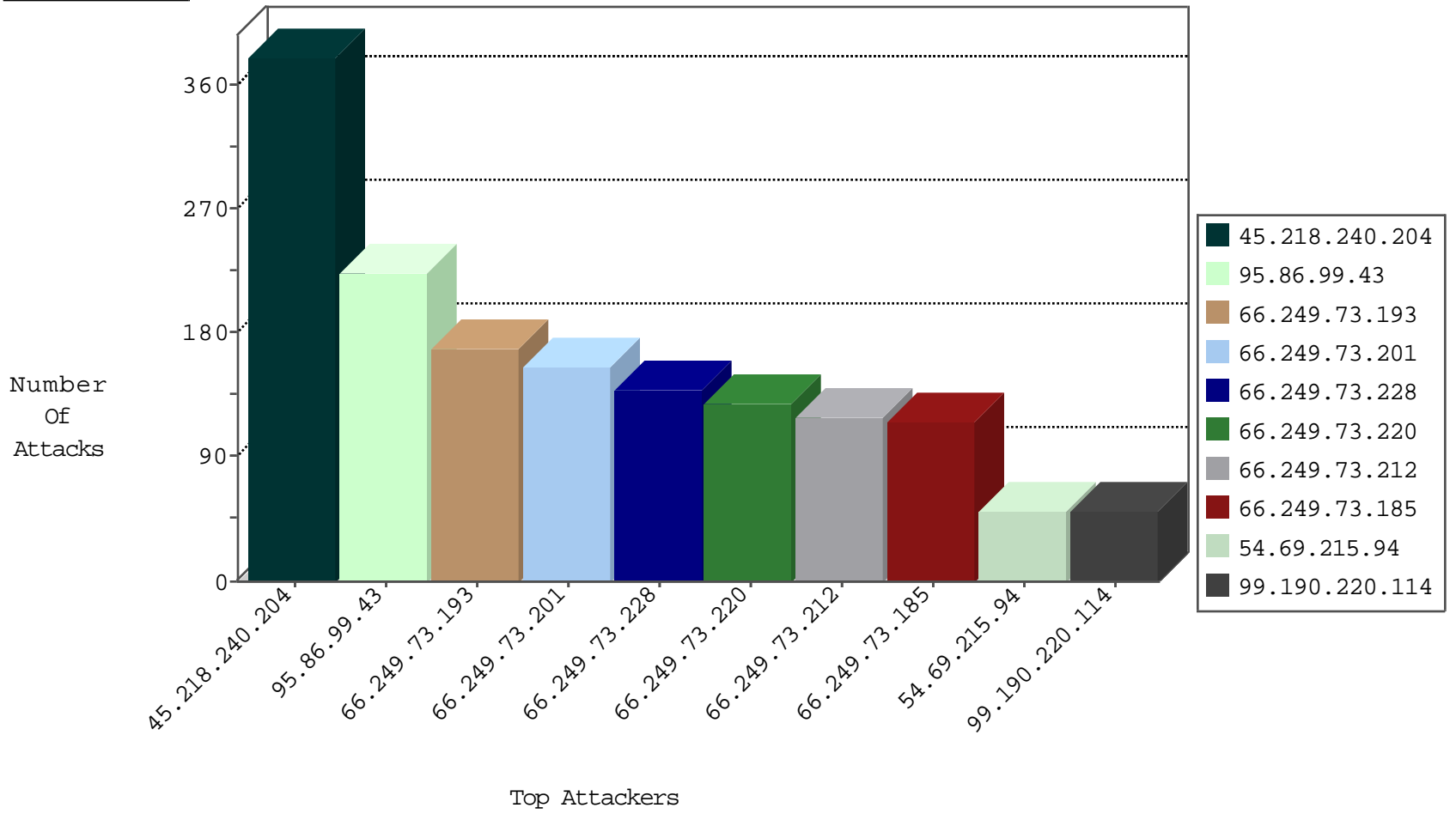




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
212.199.182.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	291
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	168
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	155
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	139
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	129
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	118
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	116
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	30
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	27
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	25
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.78.111	United States	147.237.77.170	maarachot.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	18
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.153	United States	147.237.72.166	aka.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
66.249.73.215	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	12
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.78.96	United States	147.237.77.74	law.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	10
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.248	United States	147.237.76.42	refuah.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	9
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.78.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.73.223	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.64.196	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.89.95	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.73.239	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5

04-09-2015-04:03:08 to 04-09-2015-05:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
202.162.215.242	Indonesia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
221.235.188.212	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.94.185.113	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
101.226.179.84	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
222.94.185.113	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.166	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.166	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.166	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.94.185.113	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.94.185.113	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.212	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.166	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.166	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.166	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.196.147.122	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
45.218.240.204		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	346
95.86.99.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	217
54.69.215.94	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
99.190.220.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
68.236.154.187	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
99.238.32.134	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
172.56.4.148	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
209.126.110.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
69.124.41.93	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
37.26.146.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
70.73.70.29	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
24.118.115.185	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
176.12.141.41	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.141.245	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
68.173.75.181	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
186.43.34.229	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
203.116.187.1	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
72.224.34.12	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
84.228.144.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
23.228.250.231	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
202.162.215.242	Indonesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
2.52.61.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
149.88.79.19	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
219.133.127.252	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
107.212.209.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
50.135.205.238	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
65.19.138.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
173.252.80.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
37.26.146.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
89.138.84.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
176.12.144.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
173.252.80.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
37.231.43.95	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
174.241.97.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
62.76.184.59	Russian Federation	147.237.77.233	atal.idf.il	SAM rule	drop	drop	3
181.64.192.73	Peru	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.99.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	4
176.12.141.202	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.141.202	Block	2
176.12.141.202	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	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
54.167.183.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
188.138.17.205	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
81.89.96.88	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
219.133.127.252	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/gilui/site/english/main_index.stm	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9064-he/refuah.aspx	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/milui/templates/inner.asp	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1218-3.stm	Block	1
101.22.191.97	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/110174.pdf/trackback/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
70.167.8.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/earth.stm	Block	1
198.20.69.74	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
176.12.137.246	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
209.6.131.122	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.12.141.162	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1