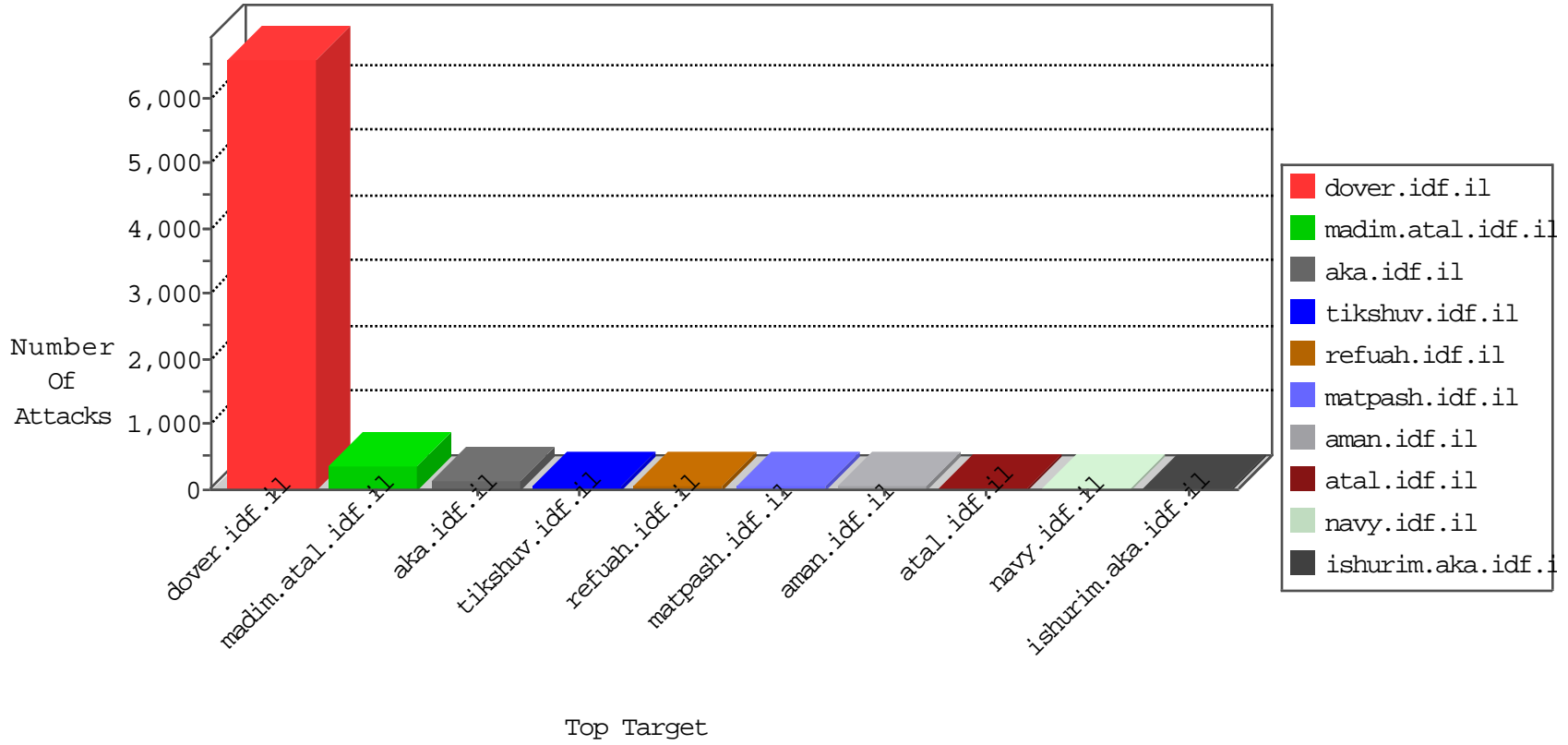
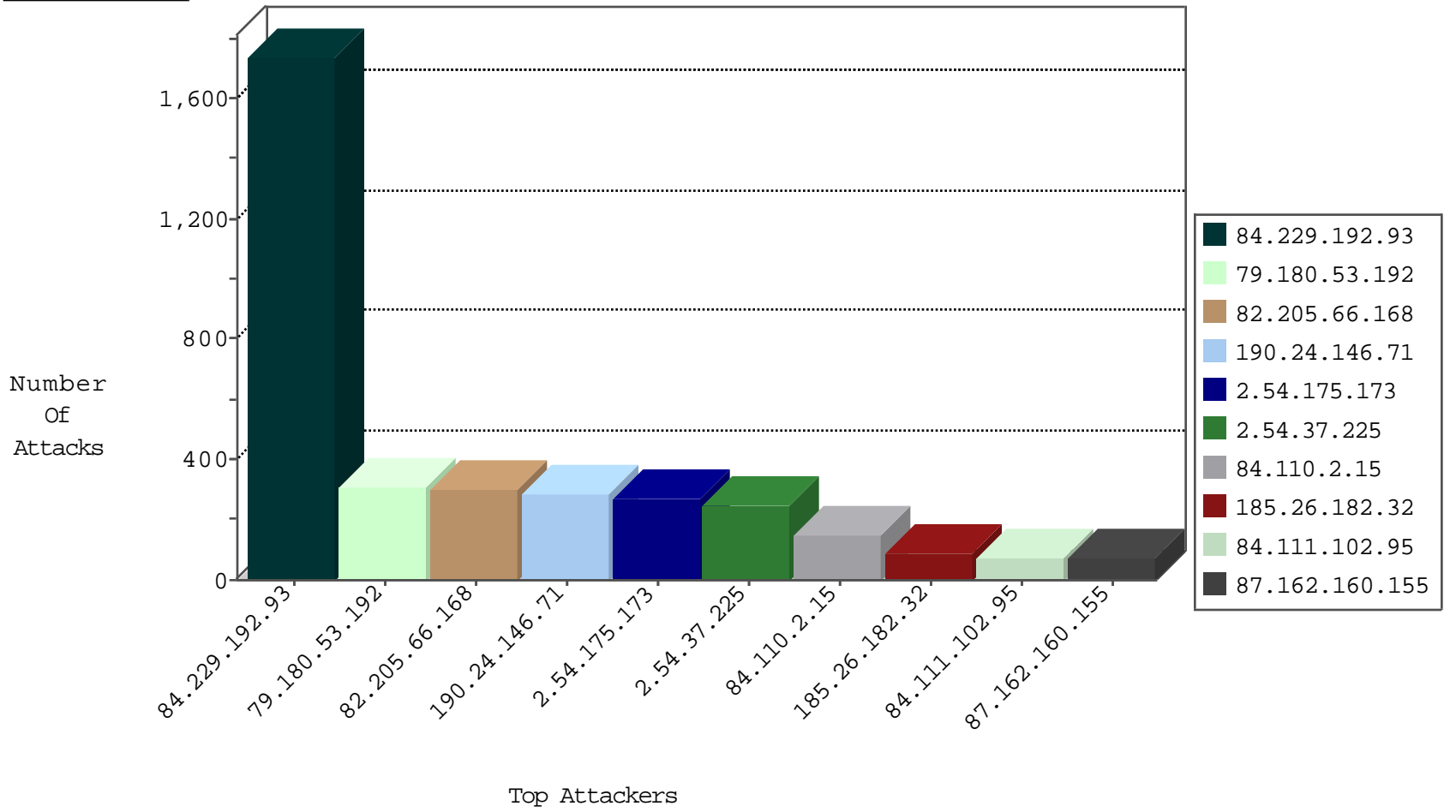




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.110.86.111	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
66.249.67.31	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	224
84.110.60.59	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
79.179.139.123	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-trafl	drop	1
49.251.234.32	Japan	147.237.76.44	e.refuah.idf.il	Block Udp_All_Nets	drop	1
62.90.207.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.64.9.223	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.142.9.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	52
37.48.74.42	Netherlands	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
37.26.148.163	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yochanan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.8	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
46.117.29.99	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
5.29.139.251	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gocenter.aka.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	19
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	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
84.110.60.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.212	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.59	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
85.65.1.78	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
146.148.9.23		147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
5.199.172.36	Lithuania	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.94.193	Singapore	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.235.188.212	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
109.66.81.189	Israel	147.237.77.216	portscan.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	Kazakstan	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
5.199.172.36	Lithuania	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.212	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
146.148.9.23		147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.212	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
5.199.172.36	Lithuania	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
117.74.137.59	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.212	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	Kazakstan	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.188.212	China	147.237.76.39	mobile.meitav.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
221.235.188.212	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
218.3.243.223	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.229.192.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1739
79.180.53.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	305
82.205.66.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	304
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	288
2.54.37.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
84.110.2.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
185.26.182.32	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	88
87.162.160.155	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
5.28.188.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
84.109.244.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
94.230.84.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
84.110.2.15	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	50
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
109.253.142.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
89.139.184.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
46.121.69.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
84.108.217.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
85.64.245.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
31.34.34.110	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
109.253.147.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
137.135.176.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
46.253.81.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
176.12.147.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.253.133.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
2.54.137.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
212.179.146.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
77.127.172.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
24.207.243.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
79.181.189.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
79.176.186.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
141.0.8.130	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.253.137.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
84.111.226.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.253.159.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
157.55.39.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
37.142.49.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
176.12.143.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
109.253.158.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
187.65.135.220	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
176.12.137.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
5.144.63.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
80.179.96.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
85.250.135.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
79.180.33.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
178.79.164.222	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.175.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	242
84.111.102.95	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.111.102.95	Block	72
2.52.33.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottonnavigaton.asp	Block	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	5
207.46.13.104	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.104	Block	5
108.59.9.143	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
84.111.129.24	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	4
216.17.46.2	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
217.195.176.194	Denmark	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
157.55.39.130	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.64.245.162	Israel	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	3
216.17.46.2	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
82.166.247.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
74.50.21.173	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
217.195.176.194	Denmark	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
114.33.42.185	Taiwan	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
198.154.240.106	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
212.48.80.60	United Kingdom	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
108.59.9.143	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
207.46.13.104	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.104	Block	2
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
85.250.253.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationervice.aspx/getuserdetails	Block	1
79.183.62.253	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
183.54.48.73	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.54.48.73	Block	1
66.249.65.28	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
36.36.176.3	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
74.50.21.173	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
89.139.35.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct117 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
183.54.48.73	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
114.33.42.185	Taiwan	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
66.249.65.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/1094-he/patzar.aspx	Block	1
37.142.164.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.151.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.104	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
94.153.8.126	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
84.110.2.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
198.154.240.106	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
66.249.67.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1681-he/refuah.aspx	Block	1
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottonnavigaton.asp	Block	1
85.64.119.110	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
77.127.243.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
212.48.80.60	United Kingdom	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1