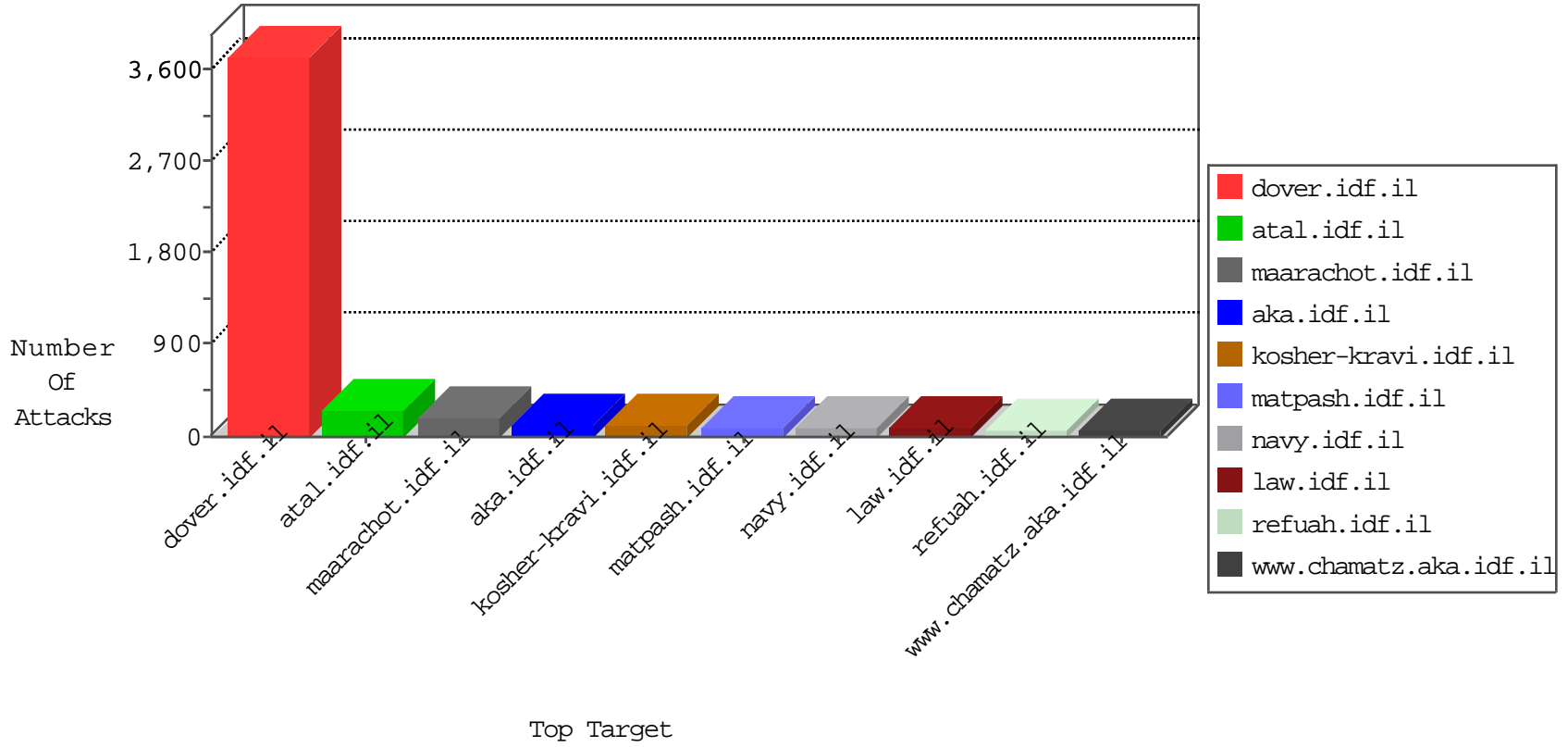
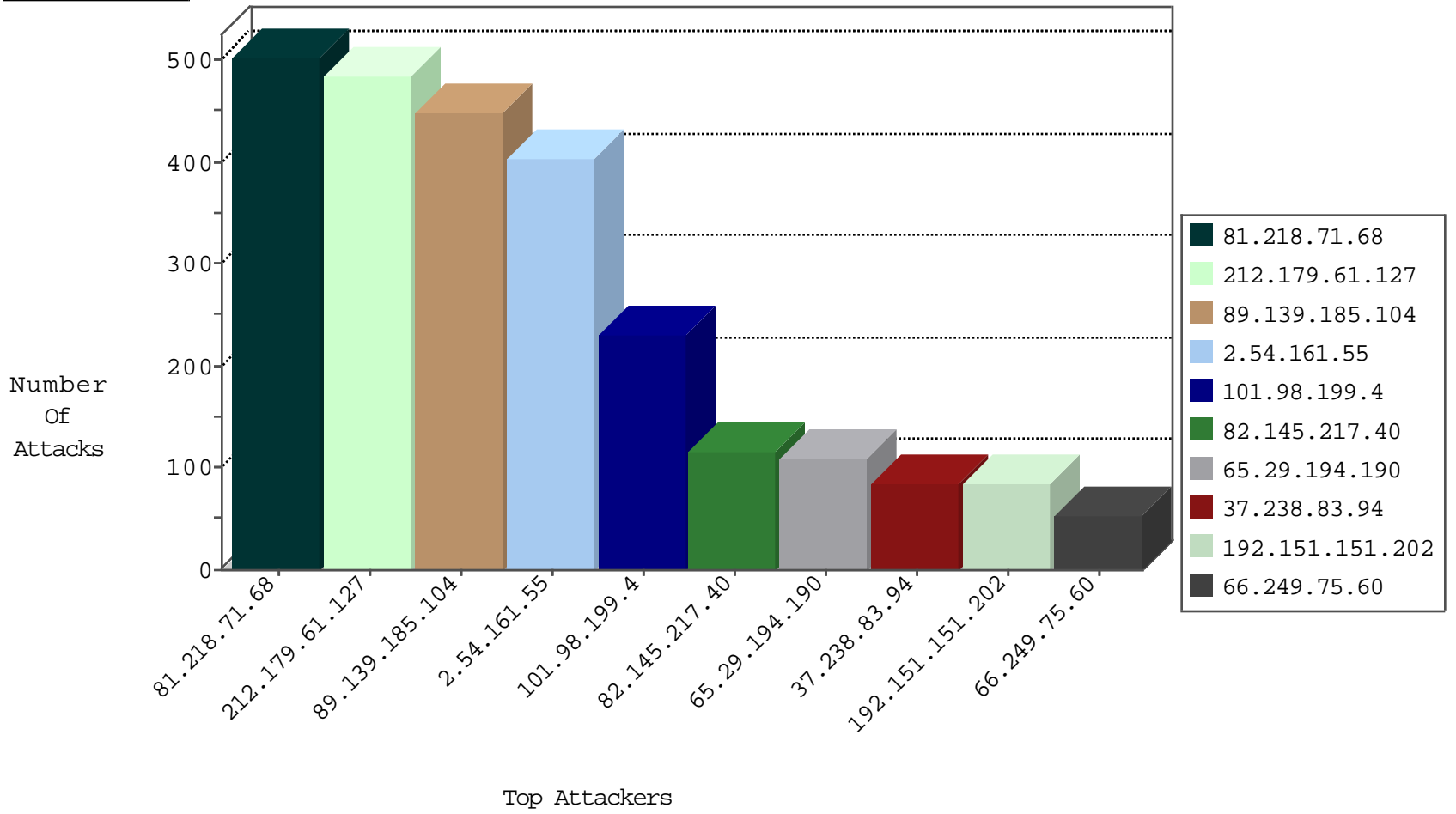


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.238.83.94	Iraq	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	289
95.151.181.91	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	94
79.182.191.74	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	76
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	52
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	51
66.249.69.74	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	41
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	37
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	35
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	34
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	32
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	31
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	29
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	29
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	26
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	26
66.249.78.97	United States	147.237.77.170	maarachot.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
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	22
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.67.39	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	18
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	17
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.67.23	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	15
66.249.64.125	United States	147.237.76.42	refuah.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	12
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.67.108	United States	147.237.77.74	law.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
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.64.27	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	9
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.31	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
82.205.1.220	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
66.249.78.61	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	7
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.75.80	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	5
66.249.79.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.64.23	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.138.57.123	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.143.147.134	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
65.29.194.190	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
37.238.83.94	Iraq	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
217.91.181.112	Germany	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
217.91.181.112	Germany	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
103.237.144.218		147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
27.50.132.61	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
217.91.181.112	Germany	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
217.91.181.112	Germany	147.237.77.243	mobile.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
217.91.181.112	Germany	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
192.64.180.14	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
94.131.14.10	Russian Federation	147.237.77.74	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
27.50.132.60	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 4096	1
69.12.92.160	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.19	madim.atal.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
81.218.71.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	503
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	484
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	446
2.54.161.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	403
101.98.199.4	New Zealand	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	230
82.145.217.40	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	116
65.29.194.190	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
109.253.158.230	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
1.179.140.114	Thailand	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
24.4.73.216	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
176.12.141.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
84.228.51.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
46.117.252.100	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
109.253.157.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
93.173.27.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
37.75.215.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
79.182.27.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
37.26.147.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
213.204.127.33	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.253.156.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
101.161.149.37	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.253.145.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
80.246.133.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
84.109.28.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
176.12.136.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
87.68.37.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
31.168.181.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
89.139.61.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
220.128.104.25	Taiwan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.150.3	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.149.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
5.22.130.27	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.149.142	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	11
109.253.131.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
176.12.149.142	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	11
109.253.136.1	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
193.106.206.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
91.228.248.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
85.250.148.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
87.68.250.0	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
188.120.148.216	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.151.151.202	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	41
192.151.151.202	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.151.151.202	Block	28
192.151.151.202	United States	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	14
192.187.126.162	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.187.126.162	Block	6
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
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
213.57.135.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/925-he/refuah.aspx	Block	1
62.219.248.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter prefixText in www.aka.idf.il/homas/site/resources/services/wsmaterials.aspx/getmaterialpossibleNamesbynamestart	None	1
192.151.151.202	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/editor/assetmanager/assetmanager.asp	Block	1
109.226.22.120	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
46.19.85.132	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	Unauthorized URL Access to www.idf.il/newsite/english/0105-3.stm	Block	1
192.187.126.162	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
109.253.136.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.225.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/gyus/login.aspx	None	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/january/0119-1.stm	Block	1
46.117.129.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
84.94.152.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
192.187.126.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fckeditor/editor/	Block	1
185.32.179.77	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.219.248.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.95.49.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.13.98.113	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4	Block	1