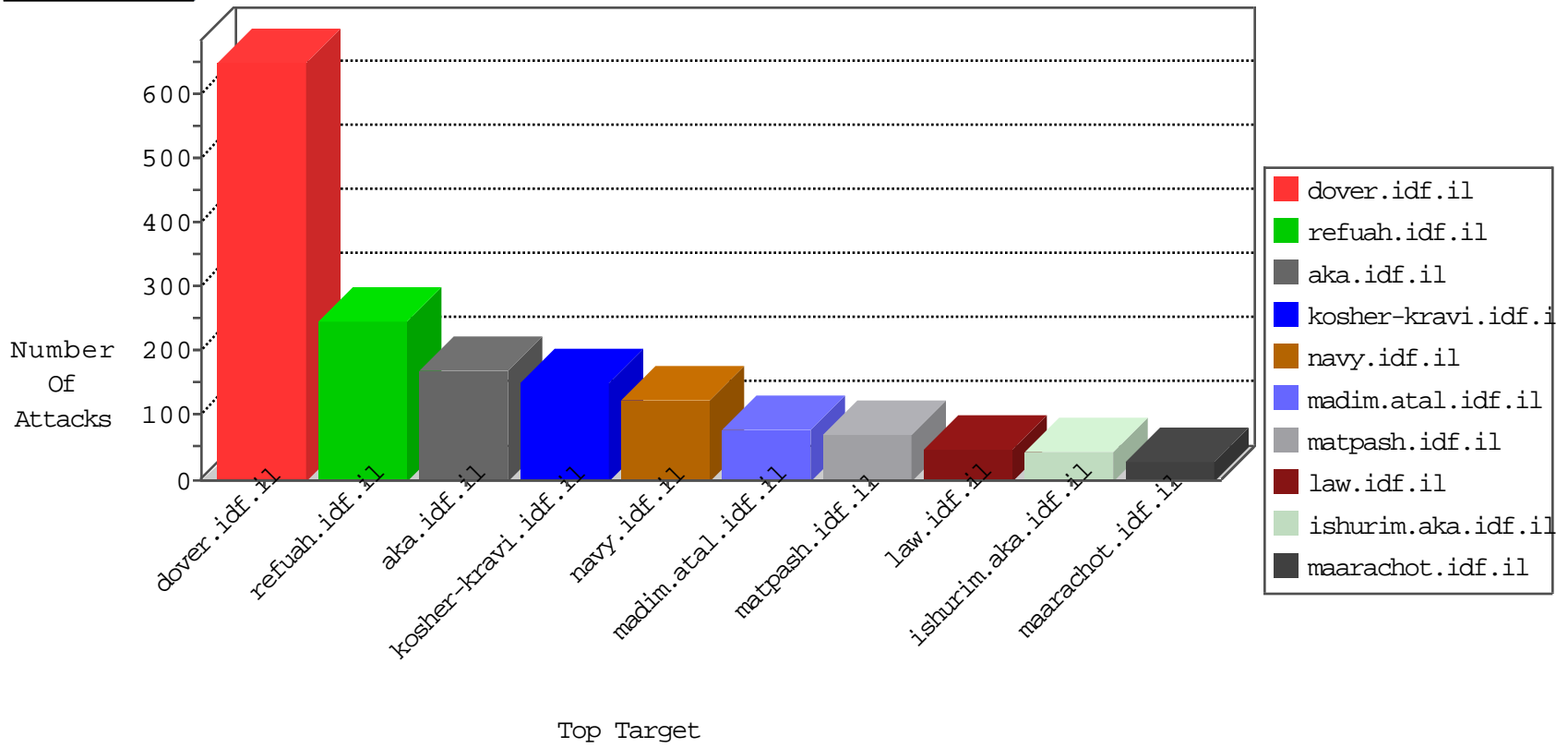
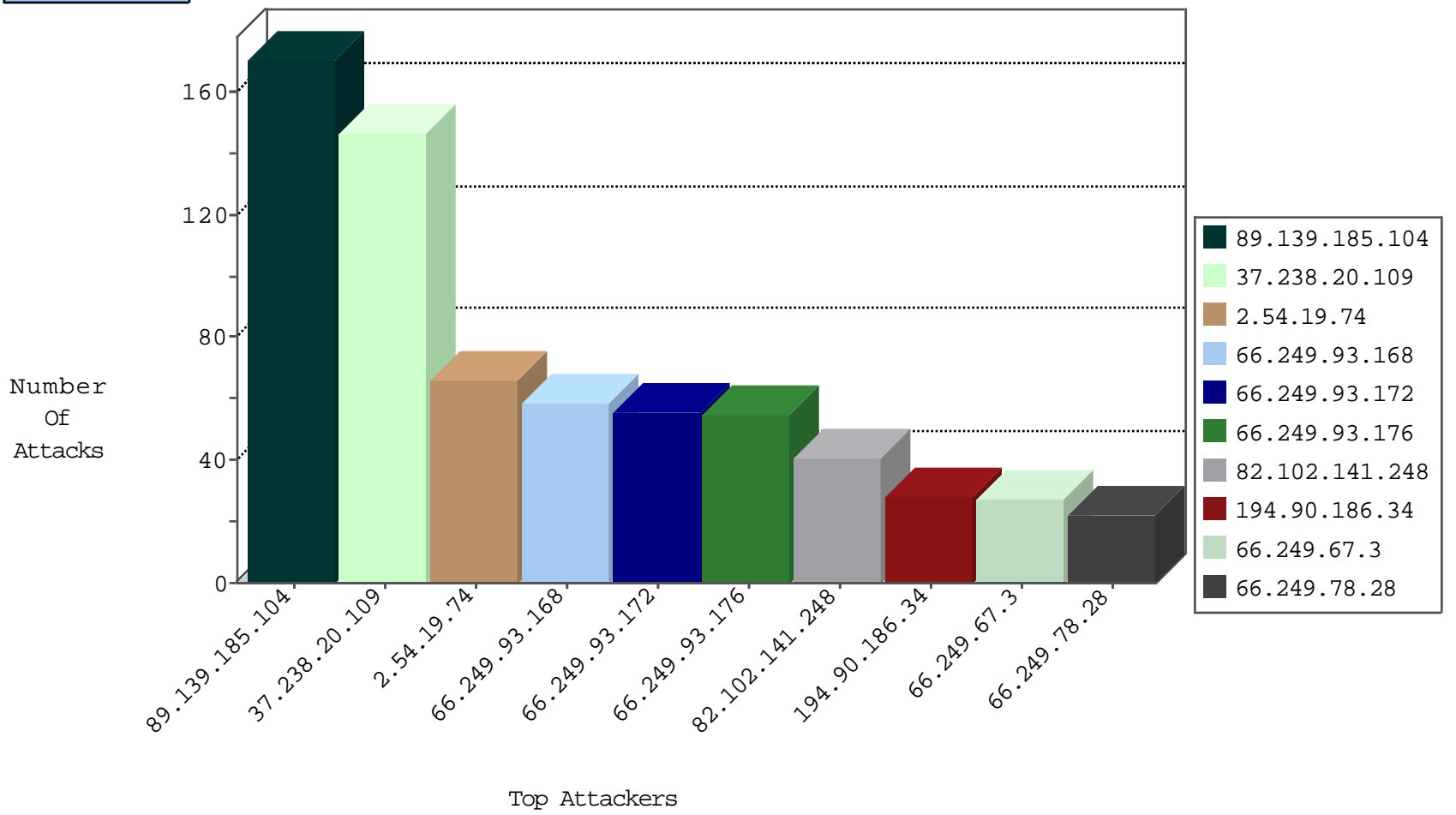


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.238.20.109	Iraq	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	538
77.125.134.81	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	130
79.183.178.210	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	120
109.65.165.89	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	65
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	59
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	56
157.55.39.6	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	56
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	55
82.102.141.248	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	41
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	27
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	22
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.67.135	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	19
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	19
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	18
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	18
62.219.151.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
46.19.86.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
66.249.78.190	United States	147.237.77.176	matpash.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
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	9
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.93.171	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	9
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.67.125	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.93.179	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	8
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.78.208	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	6
82.102.141.249	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.81.138	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.64.155	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.65.169	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ip_Web_In	drop	5
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
188.249.145.212	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
132.72.233.7	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
85.64.150.30	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.235.62.104	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
2.54.45.231	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.139.182.14	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
213.57.109.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.26.148.159	Israel	147.237.72.167	ishurim.aka.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
192.115.88.205	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
2.54.129.86	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
31.168.136.9	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	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
37.238.20.109	Iraq	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
61.240.144.67	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.194.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
5.28.172.91	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.30.85	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
120.194.36.152	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
120.194.36.152	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.126.166	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.12.141.84	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
120.194.36.152	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
120.194.36.152	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
120.194.36.152	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.68.149.59	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	170
194.90.186.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
176.12.146.82	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.150.155.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.253.156.58	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
80.179.223.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.116.190.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
193.169.70.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.142.53.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.116.203.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
176.12.151.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.109.206.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.177.173.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.26.147.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.177.118.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.121.253.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
91.199.69.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.118.30.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.99.12.99	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
81.218.131.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.178.138.115	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.172.137.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.86.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.130.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
62.219.151.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.117.128.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
88.203.16.129	Malta	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.235.22.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.23	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
80.74.105.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.180.201	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.130.248.6	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
212.235.98.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.32.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.143.166.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.138.46.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.181.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.78.119.20	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.174	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.19.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
147.236.113.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	6
109.253.138.177	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
2.52.44.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.14.184	Israel	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
93.173.149.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
77.126.69.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
150.101.164.93	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.86.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.253.129.99	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il//categorytemplates/listchilddocuments/1071	Block	1
192.99.13.139	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.181.121.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
50.87.119.130	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.67	Block	1
5.153.10.228	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
87.78.119.20	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
212.179.42.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/brothers/klali/	None	1
178.208.53.54	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
151.236.44.13	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
46.116.190.140	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
195.244.23.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter moduleT.oGoTo in www.aka.idf.il/main/giyus/login.aspx	None	1
81.201.128.70	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
176.12.143.39	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	1
41.185.27.123	South Africa	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
149.88.8.210	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.88.8.210 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
216.246.23.156	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
182.160.160.210	Australia	147.237.77.74	law.idf.il	Admin Blocking	Block	1
151.236.44.13	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.120.175.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.10.3	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
109.253.156.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
210.7.48.101	Australia	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
81.201.128.70	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
61.135.190.199	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
176.12.143.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.185.27.123	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
149.88.8.210	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
216.246.23.156	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
182.160.160.210	Australia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
155.94.222.12		147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
46.120.175.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	1
109.253.158.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
210.7.48.101	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
82.80.23.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	1
62.219.248.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTVALIDATION in aka.idf.il/main/sachar/	None	1
176.12.144.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
150.101.164.93	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1