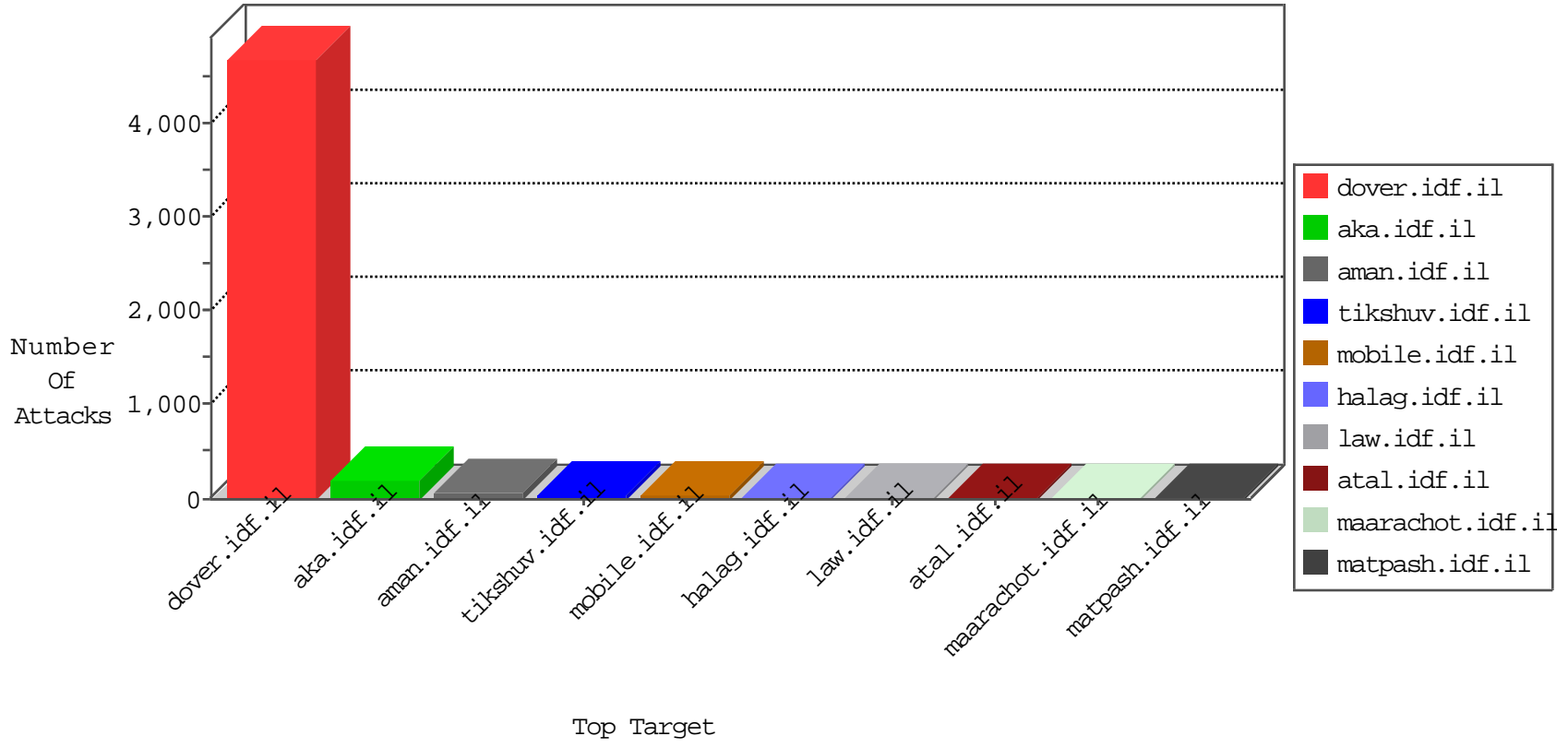
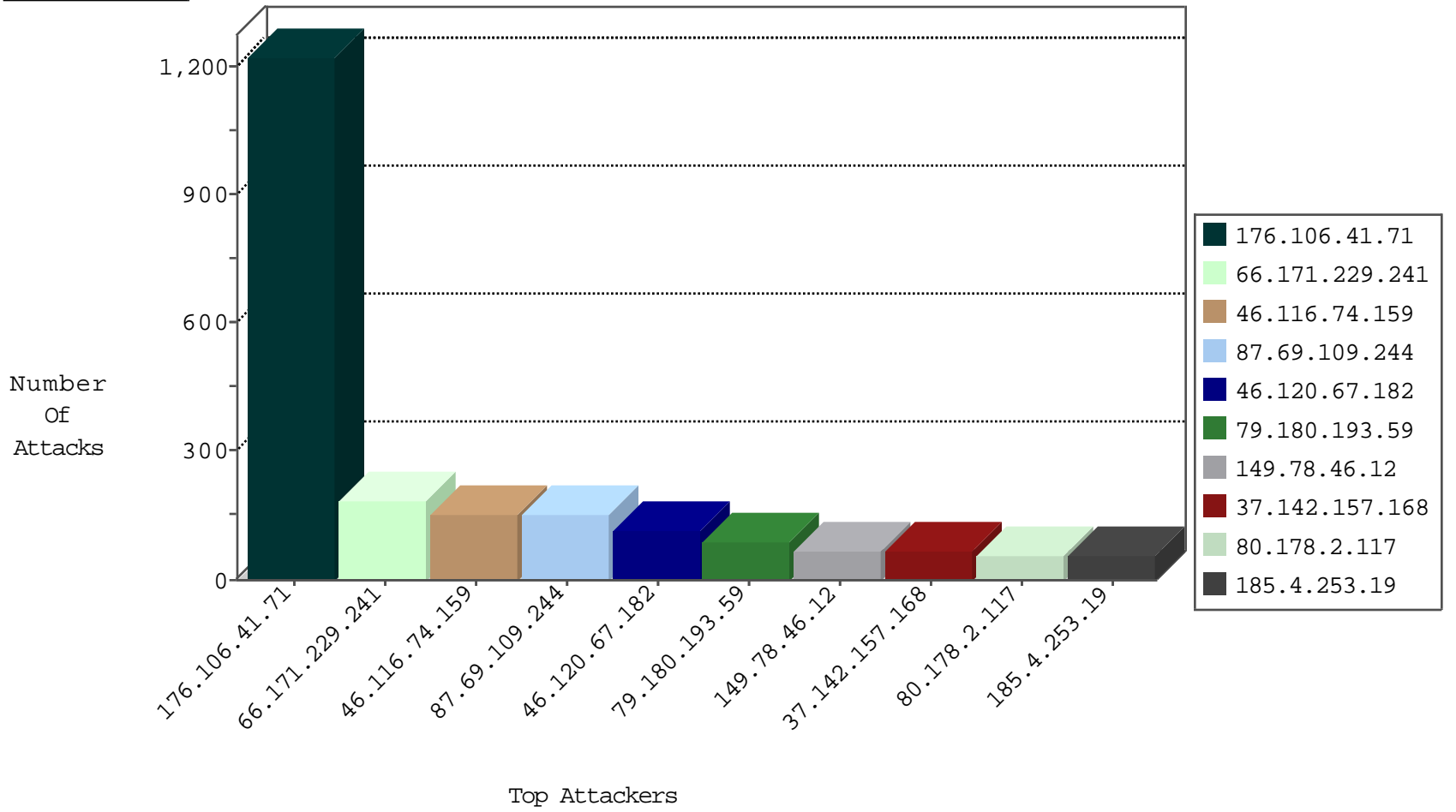




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	329
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
2.54.60.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
124.232.142.220	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
93.120.27.62	Romania	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.60	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.28	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
80.246.139.85	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
178.217.187.39	Poland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.200	mAu.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.ychalan.idf.il	DVRep_B-N_60_100	Block	1
188.120.151.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
78.193.32.48	France	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
46.120.220.109	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
89.139.169.117	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
79.178.198.34	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.ychalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
109.253.124.39	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
79.183.200.192	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
149.78.223.180	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.210	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.72.166	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
176.106.41.71	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1223
66.171.229.241	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	183
46.116.74.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	153
87.69.109.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	152
46.120.67.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	117
79.180.193.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
149.78.46.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
37.142.157.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
80.178.2.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
46.121.214.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
2.54.55.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
2.54.42.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
79.179.186.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
2.52.133.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
149.78.252.176	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
176.12.139.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
79.178.105.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
46.19.86.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
79.178.139.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
46.210.126.134	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
94.100.22.122	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
37.26.147.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
87.68.21.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
109.253.159.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
93.173.48.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.19.85.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.158.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
41.190.14.59	Nigeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
67.239.76.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
173.182.158.183	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
79.181.183.48	Israel	147.237.0.34	tikshuv.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	24
79.181.183.48	Israel	147.237.0.34	tikshuv.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	24
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
176.12.144.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
84.228.108.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
207.250.175.7	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
162.243.2.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
89.139.165.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
84.109.153.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
79.181.21.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.250.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	5
79.183.175.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
68.233.252.99	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
151.236.44.13	United Kingdom	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
46.117.194.172	Israel	147.237.76.30	himush.idf.il	Suspicious Response Code	Block	2
92.61.39.239	Lithuania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
5.9.152.78	Germany	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
37.59.222.130	France	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
216.246.23.156	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
86.109.10.1	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
109.237.211.114	Netherlands	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
66.249.73.203	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.73.203	None	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
66.249.65.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
216.246.23.156	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
109.186.82.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.aspx/getuserdetails	Block	1
46.121.205.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
86.109.10.1	Netherlands	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
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	1
157.55.39.247	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.67.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
46.117.194.172	Israel	147.237.76.30	himush.idf.il	Unauthorized Method POST for www.chimush.atal.idf.il/1324-he/himush.aspx	None	1
93.173.1.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.212.108	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
80.246.130.166	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.237.211.114	Netherlands	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
37.142.226.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/default.asp	Block	1
176.12.143.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
46.117.194.172	Israel	147.237.76.30	himush.idf.il	Unknown Parameter fromDate in www.chimush.atal.idf.il/1325-he/himush.aspx	None	1
104.222.192.139		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
85.214.251.131	Germany	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
5.102.173.71	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/jump_0900.stm	Block	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
89.139.165.232	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
41.248.22.75	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/login	Block	1
79.177.107.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
176.12.150.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.194.172	Israel	147.237.76.30	himush.idf.il	Unknown Parameter searchText in www.chimush.atal.idf.il/1324-he/himush.aspx	None	1
109.64.116.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 1429357433813 in www.aka.idf.il/main/giyus/login.aspx	None	1
85.214.251.131	Germany	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
68.233.252.99	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
151.236.44.13	United Kingdom	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
66.249.64.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1