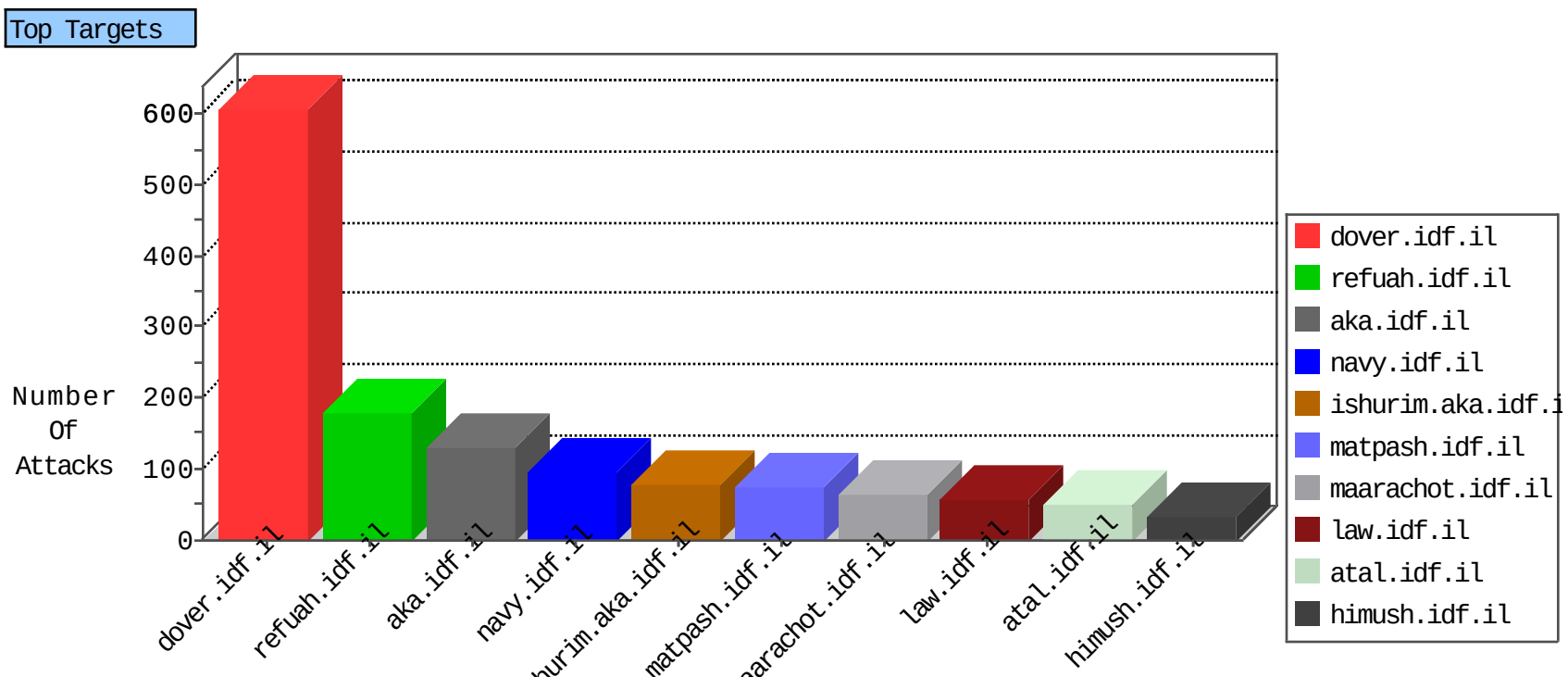
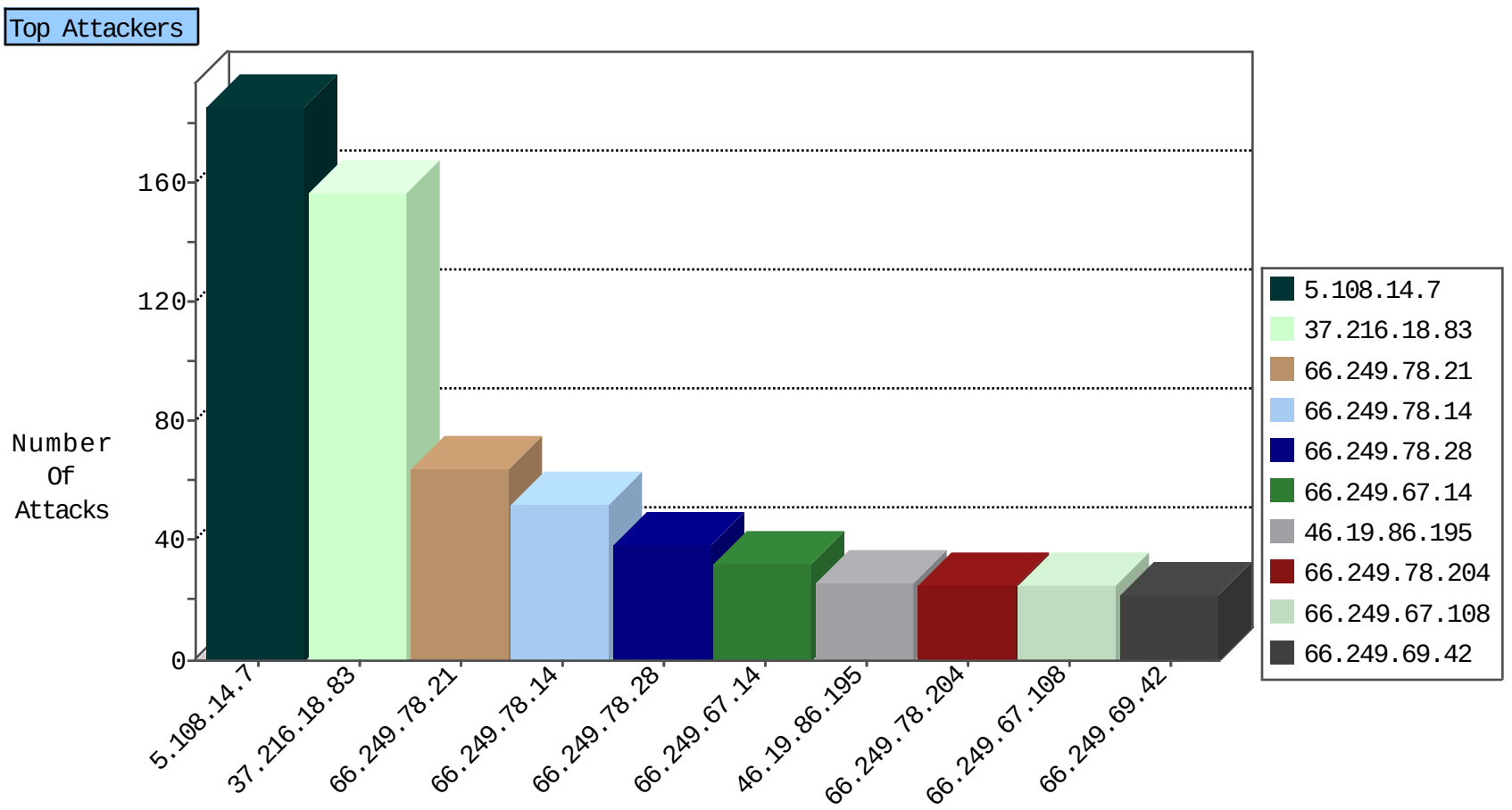
04-12-2015-06:03:01 to 04-12-2015-07:03:01

IDF Under Attack
04-12-2015-06:03:01

Top Targets



Top Attackers



04-12-2015-06:03:01 to 04-12-2015-07:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.86.195	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	64
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	52
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	39
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	32
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	25
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	25
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.78.215	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	14
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	14
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.78.222	United States	147.237.72.167	ishurim.aka.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	12
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.64.87	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	12
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.78.208	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	12
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.65.196	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	11
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.93.144	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	9
66.249.93.152	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	9
66.249.81.212	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.58	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	8
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.64.155	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.64.63	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.78.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.69.17	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5

04-12-2015-06:03:01 to 04-12-2015-07:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
27.123.171.88	Fiji	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.181.15.94	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-12-2015-06:03:01 to 04-12-2015-07:03:01

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	6
43.255.191.170	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
213.26.203.138	Italy	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
168.235.154.235		147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 4096	1
27.50.132.60	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
54.224.149.230	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
43.255.191.170	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.170	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
213.26.203.138	Italy	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.170	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

04-12-2015-06:03:01 to 04-12-2015-07:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.108.14.7	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	186
37.216.18.83	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	157
71.235.33.244	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
46.19.86.195	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	17
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
189.217.7.114	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
216.154.98.97	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
27.123.171.88	Fiji	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.19.85.84	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.122.74.184	Ukraine	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
84.110.54.33	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	4
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
120.28.109.84	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.153	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.84	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.154.17.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
122.60.81.15	New Zealand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
84.110.54.33	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	alert	3
173.252.110.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.121.14.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.176.35.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
178.254.10.124	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
173.252.74.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.0.66.65	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.26.146.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.250.189.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.89	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
73.212.43.132	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
173.252.74.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
158.222.13.72		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
180.234.127.112	Bangladesh	147.237.0.19	madim.atal.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
46.116.111.95	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
164.138.23.97	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
134.129.203.28	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	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
96.30.2.168	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
216.246.23.156	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
77.122.74.184	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
197.38.239.128	Egypt	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/80	Block	1
180.234.127.112	Bangladesh	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
142.4.200.219	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.214.16.223	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
67.214.126.180	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
192.169.59.190	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
37.187.50.84	France	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
134.249.53.8	Ukraine	147.237.77.216	dover.idf.il	Web leech 9	Block	1
198.46.88.119	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
77.122.74.184	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
180.234.127.112	Bangladesh	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
31.168.220.100	Israel	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/default.asp	Block	1
207.46.13.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.89	Block	1
91.103.217.26	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
67.214.126.180	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
192.169.59.190	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
173.252.120.118	United States	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.15//80	Block	1
37.187.50.84	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
142.4.200.219	Canada	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
198.46.88.119	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
79.183.108.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.x in www.aka.idf.il/main/sachar/	None	1
184.107.143.138	Canada	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
52.1.33.44	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
31.168.220.100	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
91.103.217.26	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
193.105.41.182	Ukraine	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
178.60.205.53	Spain	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
46.19.85.84	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
142.4.200.219	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
200.73.3.163	Chile	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
84.229.42.158	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storag	Block	1
184.107.143.138	Canada	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
54.207.82.68	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
31.193.51.84	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.102	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/9/110539.pdf,	Block	1
96.30.2.168	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
216.246.23.156	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
193.105.41.182	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1