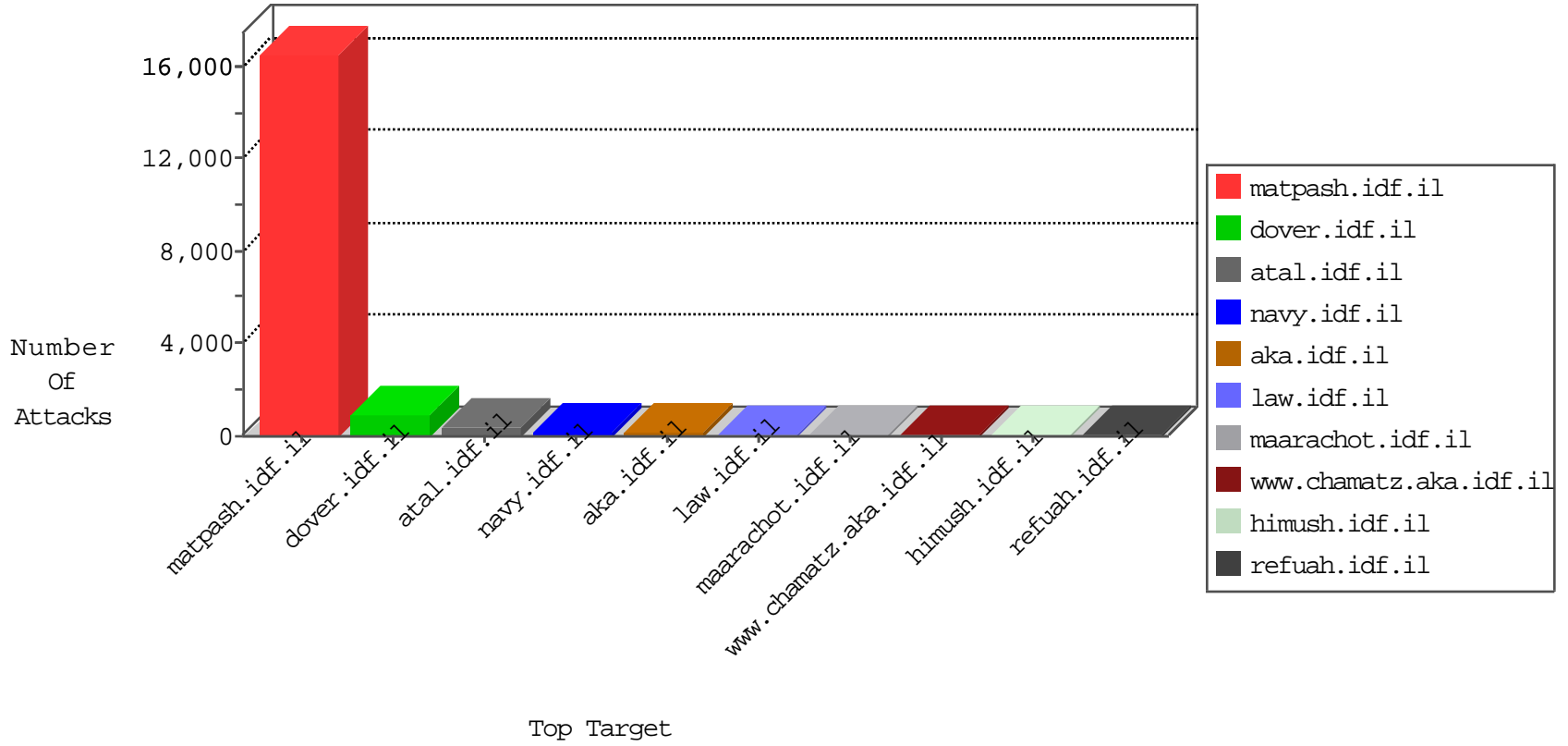
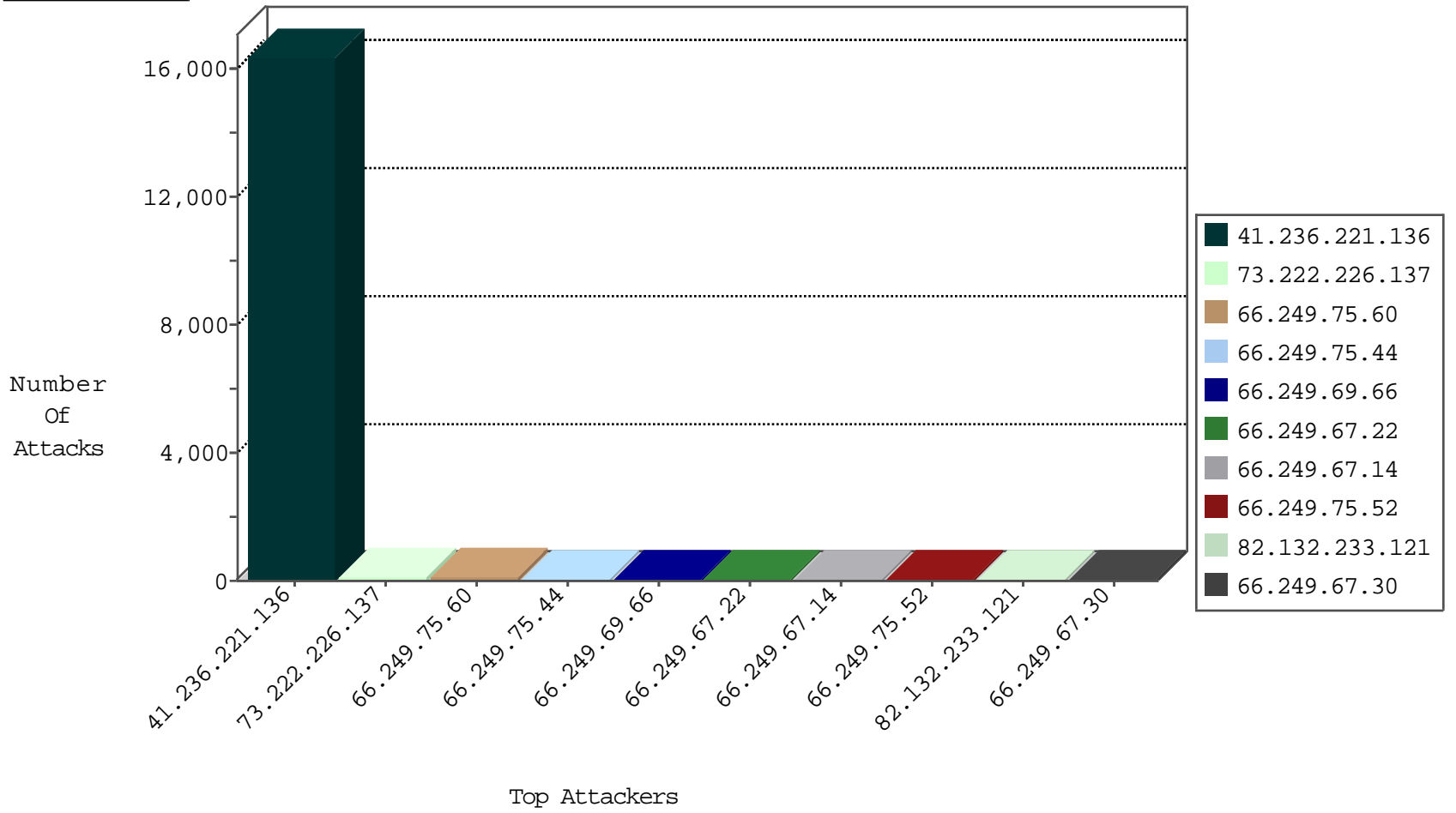


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	75
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	69
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	68
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	65
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	61
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	56
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	54
66.249.69.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	47
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	44
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	40
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	38
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	36
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	34
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	31
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	24
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	21
66.249.64.27	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	21
66.249.78.166	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	15
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.64.23	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	14
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.64.19	United States	147.237.76.30	himush.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
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.141	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
46.120.31.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
72.69.81.60	United States	147.237.77.176	matpash.idf.il	network flood IPv4 ICMP	drop	6
66.249.64.38	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.18	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.64.124	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.75.78	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	4
175.141.27.228	Malaysia	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	4
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.67.23	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.78.76	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
67.18.208.240	United States	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	5
174.20.136.211	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
43.255.191.163	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
213.136.84.245	Germany	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
194.78.216.163	Belgium	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
213.136.84.245	Germany	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
194.78.215.226	Belgium	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.236.221.136	Egypt	147.237.77.176	matpash.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	16392
73.222.226.137	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
82.132.233.121	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
75.172.80.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
24.152.254.19	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
79.181.142.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
174.20.136.211	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
208.54.45.196	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
24.107.145.132	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
173.24.207.73	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
185.13.193.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
64.234.59.241	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
149.78.80.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
151.203.17.38	United States	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.86.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
70.72.184.255	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
104.50.97.14		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
71.197.177.254	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.236.221.136	Egypt	147.237.77.176	matpash.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	8
84.228.87.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
209.133.111.211	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
149.78.80.210	Israel	147.237.77.243	mobile.idf.il	First packet isn't SYN	drop	drop	8
91.200.12.28	Ukraine	147.237.77.74	law.idf.il	SAM rule	drop	drop	7
46.19.123.125	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
70.210.49.163	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
92.25.208.93	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
151.203.17.38	United States	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.120.31.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
87.69.79.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.176.4.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
98.17.13.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
92.241.53.84	Jordan	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
74.110.151.186	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
188.165.15.241	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
89.139.178.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
190.181.201.93	Honduras	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.154.7.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

04-08-2015-02:03:08 to 04-08-2015-03:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
109.66.10.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
207.46.13.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.120.31.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
23.20.72.246	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8896-he/refuah.aspx	Block	1
92.27.98.11	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.79	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.236.221.136	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	1
207.46.13.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1360-he/atal.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
114.112.90.54	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
213.251.182.12	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
180.76.6.51	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/1048-7536-he/tikshuv.aspx	Block	1
79.180.198.55	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
151.203.17.38	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
188.138.17.205	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
80.246.136.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/logi	Block	1

04-08-2015-02:03:08 to 04-08-2015-03:03:08