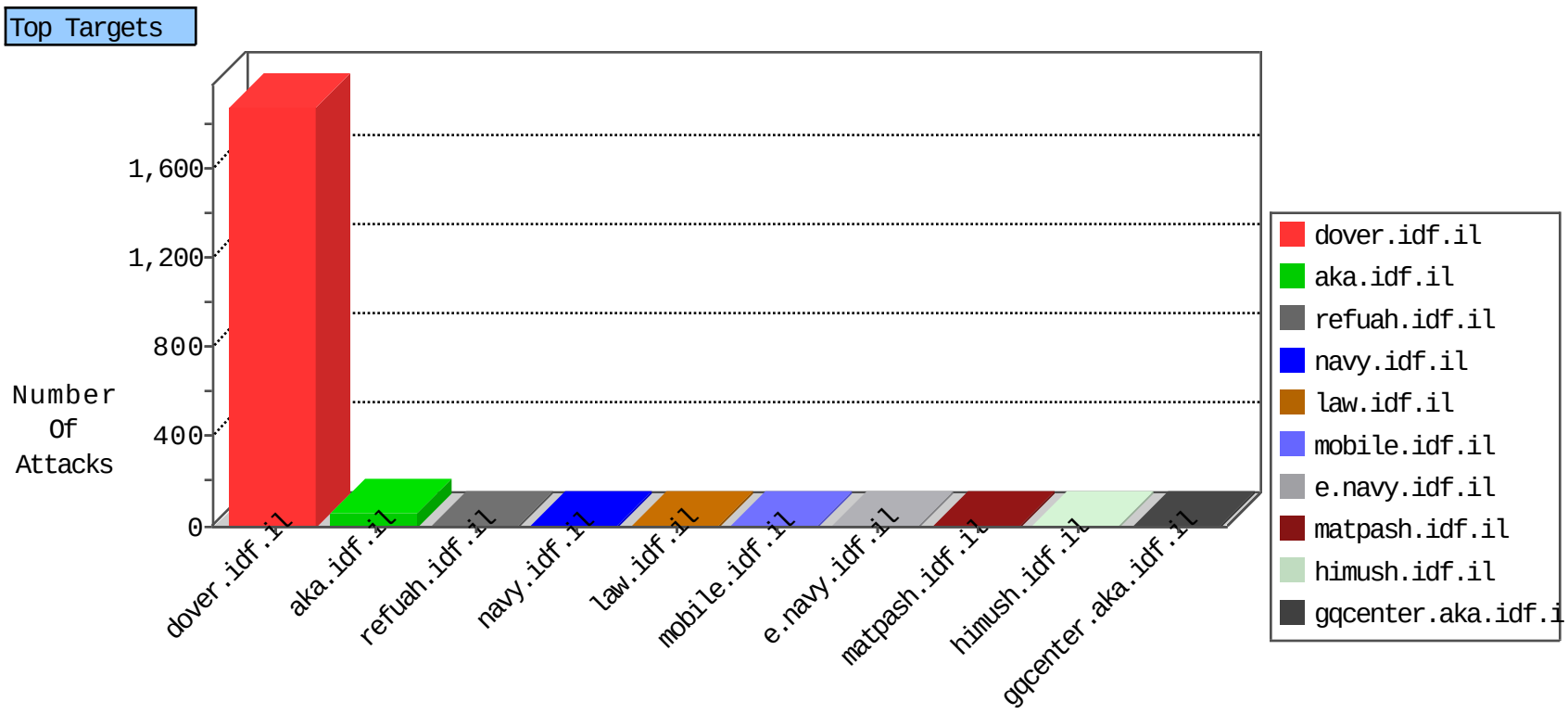
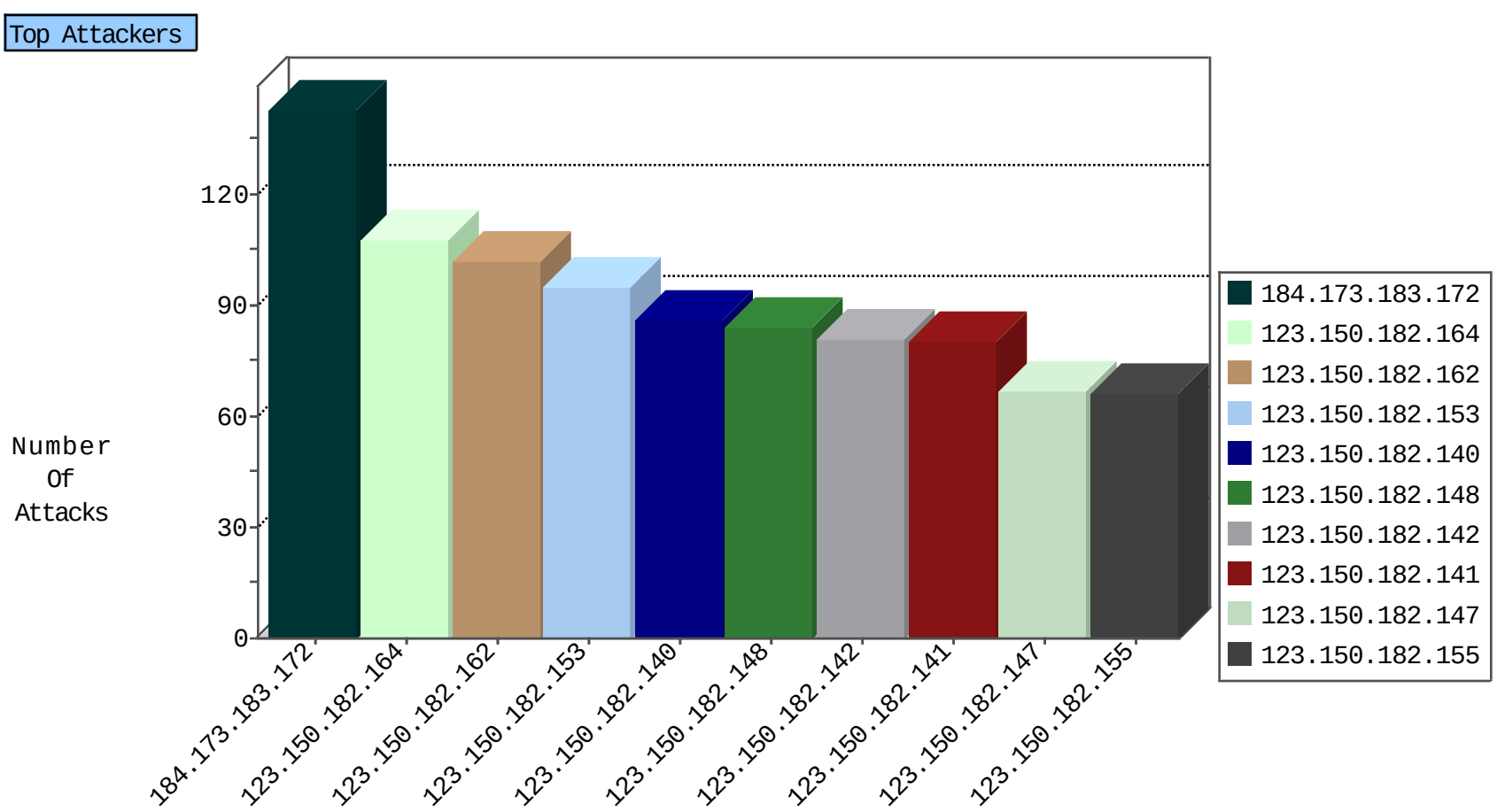
05-11-2015-03:03:08 to 05-11-2015-04:03:08

IDF Under Attack
05-11-2015-03:03:08

Top Targets



Top Attackers



05-11-2015-03:03:08 to 05-11-2015-04:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.104	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2972
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	214
220.181.108.176	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	110
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	10
124.232.142.220	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

05-11-2015-03:03:08 to 05-11-2015-04:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	143
85.25.43.94	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.139	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	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.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
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	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.201	e.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
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1

05-11-2015-03:03:08 to 05-11-2015-04:03:08

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	7
121.88.5.177	Korea, Republic of	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.205.123	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.205.123	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
8.29.144.205	United States	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
178.19.107.114	Poland	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.0.60	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.205.123	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
208.124.237.146	Canada	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
8.29.144.205	United States	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
182.18.162.15	India	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
8.29.144.205	United States	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -f -sS	1
144.0.0.60	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
144.0.0.60	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1

05-11-2015-03:03:08 to 05-11-2015-04:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
123.150.182.164	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
123.150.182.162	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	102
123.150.182.153	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	95
123.150.182.140	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	86
123.150.182.148	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
123.150.182.142	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
123.150.182.141	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
123.150.182.147	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
123.150.182.155	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
123.150.182.149	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
123.150.182.157	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
123.150.182.145	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
123.150.182.163	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
186.124.7.197	Argentina	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
123.150.182.146	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
2.54.157.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
123.150.182.144	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
123.150.182.160	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
123.150.182.154	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
123.150.182.150	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
66.249.73.201	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
123.150.182.151	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
123.150.182.143	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
95.86.110.87	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
123.150.182.152	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
123.150.182.156	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	18
46.19.85.216	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
46.19.85.89	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
79.154.88.34	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
17.142.152.86	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
17.142.152.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
69.162.139.9	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
220.255.1.169	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
221.192.179.48	China	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
99.234.222.250	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
17.142.152.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
17.142.152.94	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
17.142.152.81	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
17.142.145.3	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
195.66.128.86	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
17.142.151.101	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.26.146.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
123.150.182.139	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
17.142.152.85	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6

05-11-2015-03:03:08 to 05-11-2015-04:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.62	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.62	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	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
157.55.39.32	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.139.17.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
2.54.182.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
67.210.119.235	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//blog/wp-admin/	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.152.128.27	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11437-en/dover.aspx/rk=0/rs=tmjq2rcickbyhjb7c261yvagera-	Block	1
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.213	Block	1
31.6.71.218	Poland	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19336-he/kkkkkkk=39b07ab9kkkkkkk_39b07ab9	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6497-he/patzar.aspx	Block	1
157.55.39.199	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
149.255.58.110	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
188.165.15.138	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
52.0.189.35	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/skira/default.asp	None	1
81.89.96.91	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/913-4475-he/patzar.aspx	Block	1
173.236.224.114	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wp/wp-admin/	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
197.242.159.201	South Africa	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wordpress/wp-admin/	Block	1
62.210.209.22	France	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//	Block	1
157.55.39.139	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.73.197	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1682	Block	1
178.137.81.145	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1283-he/refuah.aspx	Block	1
66.249.64.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.144	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
107.20.201.73	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1

05-11-2015-03:03:08 to 05-11-2015-04:03:08