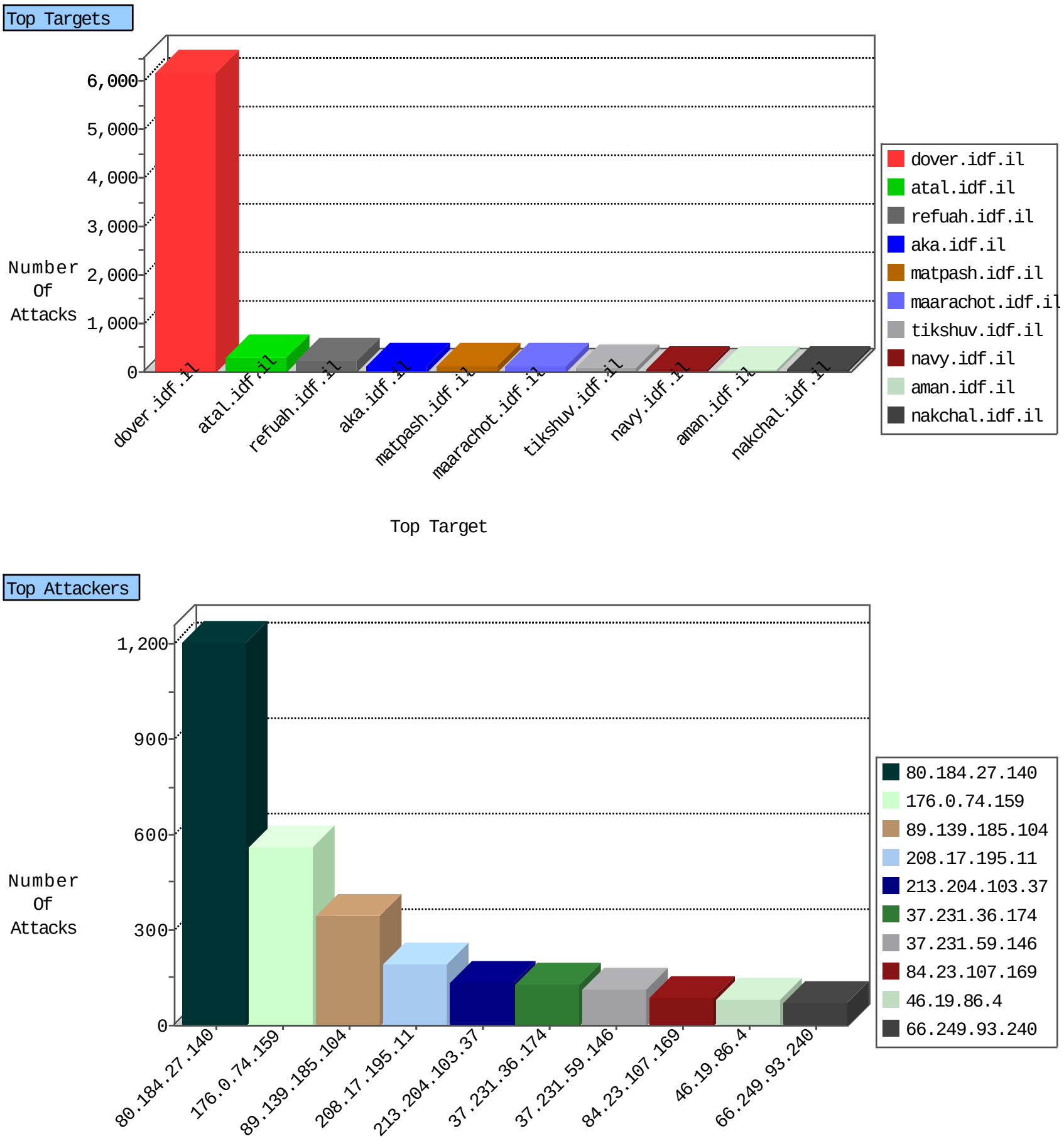
04-08-2015-18:03:05 to 04-08-2015-19:03:05

IDF Under Attack
04-08-2015-18:03:05



04-08-2015-18:03:05 to 04-08-2015-19:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	284
46.117.190.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
87.69.234.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
109.66.41.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
157.55.39.41	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	89
66.249.93.240	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	73
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	65
66.249.93.243	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	63
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	60
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	59
66.249.93.246	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	46
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	31
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	30
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	30
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	25
66.249.69.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	24
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	20
66.249.64.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	19
66.249.93.235	United States	147.237.0.34	tikshuv.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	19
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	18
66.249.93.179	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.81.189	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	14
66.249.64.23	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	13
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.93.175	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.78.148	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	13
66.249.67.159	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	12
66.249.81.233	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.67.39	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	11
66.249.67.84	United States	147.237.77.74	law.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	11
208.17.195.11	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.67.151	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.64.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.78.141	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.93.234	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7

04-08-2015-18:03:05 to 04-08-2015-19:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.125.161.29	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
188.120.153.123	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
92.243.183.14	Russian Federation	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.82.70.198	Netherlands	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	1
77.125.88.139	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	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
80.82.70.198	Netherlands	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	1
84.109.203.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.186.93.76	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.76.38	e.e.meitav.idf.il	DVRep_P-N_40-59	Permit	1
87.197.141.115	Slovakia	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.8.24	e.lifestyle.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.76.202	e.halag.idf.il	DVRep_P-N_40-59	Permit	1
2.54.142.125	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.8.45	e.eitan.idf.il	DVRep_P-N_40-59	Permit	1

04-08-2015-18:03:05 to 04-08-2015-19:03:05

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	8
79.125.161.29	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
43.255.191.141	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.101.21.179	Russian Federation	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.101.21.179	Russian Federation	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.101.21.179	Russian Federation	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
46.101.21.179	Russian Federation	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
208.124.237.146	Canada	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
185.23.127.250	Bahrain	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.141	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

04-08-2015-18:03:05 to 04-08-2015-19:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
80.184.27.140	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1207
176.0.74.159	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	563
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	344
208.17.195.11	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	191
213.204.103.37	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
37.231.36.174	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	128
37.231.59.146	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	112
84.23.107.169	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	86
46.19.86.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	79
213.57.139.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	68
176.19.148.54	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
188.236.89.184	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
46.19.85.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
121.54.54.250	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
134.192.85.29	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
84.228.249.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
46.19.86.235	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
168.187.42.103	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
199.58.86.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
84.235.85.68	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
188.140.181.100	Oman	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
212.71.254.234	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
188.70.142.153	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
77.127.144.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
89.138.83.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
94.200.220.251	United Arab Emirates	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
2.52.46.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
67.2.225.223	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
77.127.53.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
109.253.132.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
77.126.151.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
74.6.254.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
31.30.81.248	Czech Republic	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
78.95.206.50	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
107.167.99.222	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
37.26.146.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
93.169.128.48	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
5.31.151.17	United Arab Emirates	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
176.12.151.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
83.244.37.98	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
109.64.101.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
62.119.166.9	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
176.12.144.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18

04-08-2015-18:03:05 to 04-08-2015-19:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
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
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.183.25.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.57.194.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.10	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5494-he/patzar.aspx	Block	1
94.159.165.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.178.8.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
50.87.119.130	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
207.241.237.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/french/info.stm	Block	1
85.250.159.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.62.93	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	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
109.66.118.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
80.184.27.140	Kuwait	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arbic	Block	1
50.87.119.130	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
210.86.239.207	Vietnam	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.51.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
79.177.201.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/021004-1.stm	Block	1
109.253.83.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
84.108.138.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.50	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
210.86.239.207	Vietnam	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
188.143.232.72	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.72	Block	1
87.197.141.115	Slovakia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.183.18.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
2.52.146.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.145.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.111.152.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
213.57.42.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
188.143.232.72	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
93.172.43.93	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.147	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
149.78.80.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
84.111.216.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1

04-08-2015-18:03:05 to 04-08-2015-19:03:05