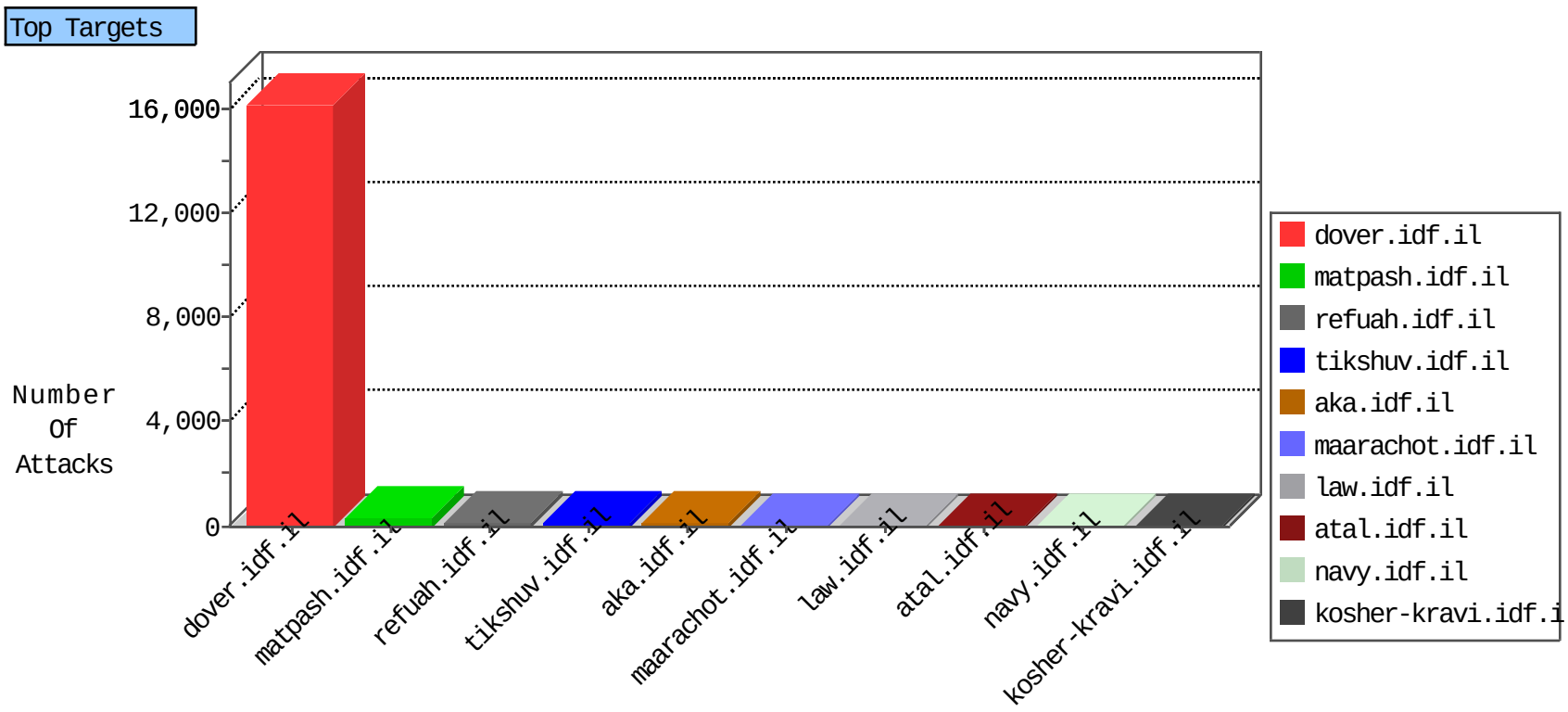
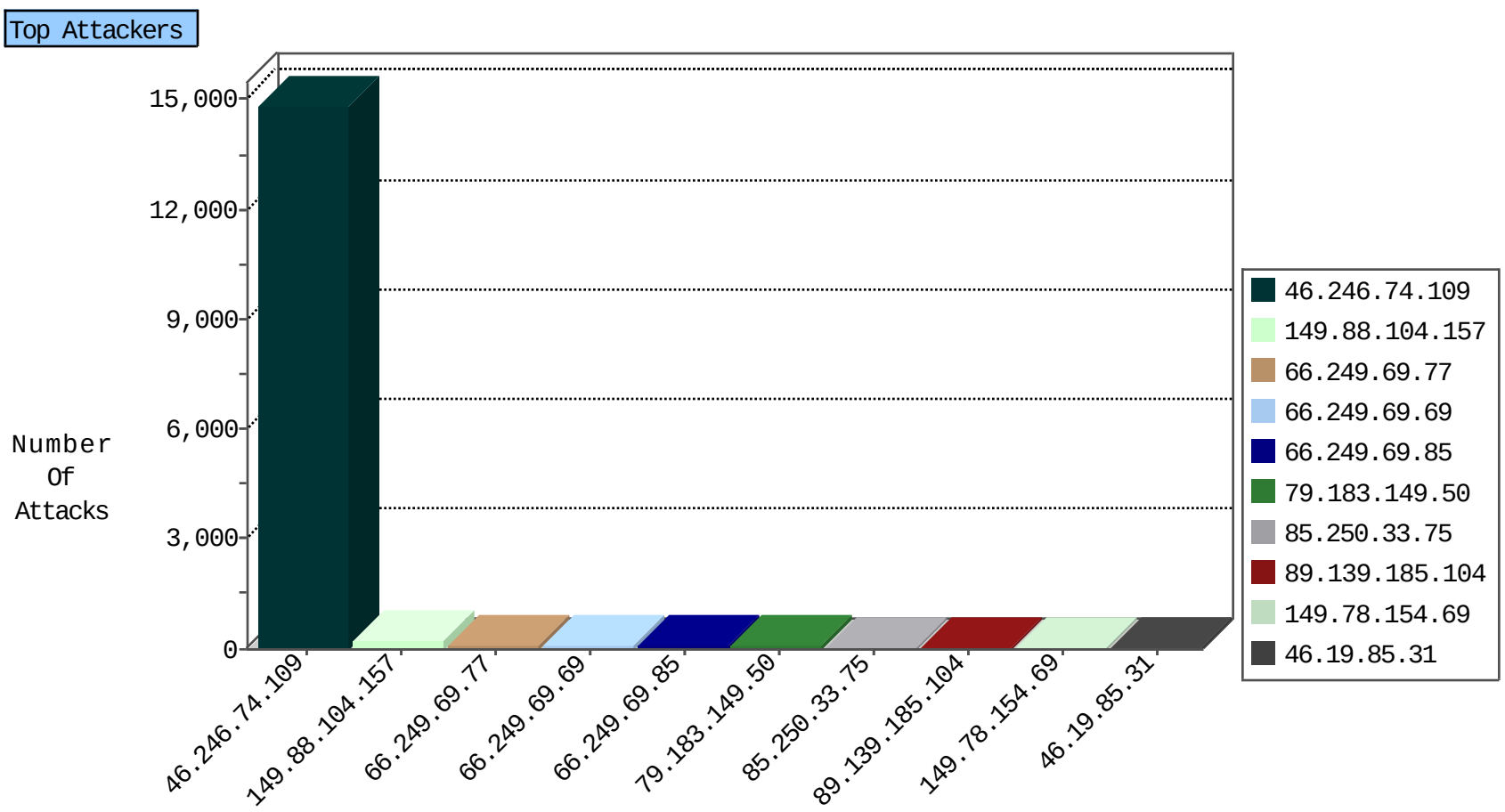
04-11-2015-09:03:09 to 04-11-2015-10:03:09

IDF Under Attack
04-11-2015-09:03:09





04-11-2015-09:03:09 to 04-11-2015-10:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	111
46.246.74.109	Sweden	147.237.77.216	dover.idf.il	HTTP-MISC-WebLogic-Str-BO	dest-reset	106
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	105
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	100
46.246.74.109	Sweden	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	65
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	40
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	25
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	22
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.248	United States	147.237.76.42	refuah.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
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.111	United States	147.237.77.170	maarachot.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
66.249.69.63	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	12
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.69.101	United States	147.237.72.166	aka.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	10
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.69.47	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.64.121	United States	147.237.76.42	refuah.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
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.69.120	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.78.134	United States	147.237.72.156	aman.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
66.249.69.97	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.69.112	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5
66.249.78.141	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4

04-11-2015-09:03:09 to 04-11-2015-10:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.246.74.109	Sweden	147.237.77.216	dover.idf.il	C1000203: HTTP: Thorshammer - Post to root dir	Block	12
205.206.103.164	Canada	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
218.6.132.45	China	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	2
37.237.128.35	Iraq	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.116.74.202	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.67.177.175	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

04-11-2015-09:03:09 to 04-11-2015-10:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
94.43.85.2	Georgia	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
94.43.85.2	Georgia	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.43.85.2	Georgia	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
213.34.193.242	Kuwait	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.243.126.2	Iran, Islamic Republic of	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
207.241.237.224	United States	147.237.72.166	aka.idf.il	WEB-CGI redirect access	1
43.255.191.165	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
94.43.85.2	Georgia	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.43.85.2	Georgia	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
94.43.85.2	Georgia	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
94.43.85.2	Georgia	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
94.43.85.2	Georgia	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
94.43.85.2	Georgia	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
213.34.193.242	Kuwait	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.165	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.243.126.2	Iran, Islamic Republic of	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
213.34.193.242	Kuwait	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.243.126.2	Iran, Islamic Republic of	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.43.85.2	Georgia	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.35	akaws.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.43.85.2	Georgia	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
94.43.85.2	Georgia	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1

04-11-2015-09:03:09 to 04-11-2015-10:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.246.74.109	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10827
46.246.74.109	Sweden	147.237.77.216	dover.idf.i	SAM rule	drop	drop	2418
46.246.74.109	Sweden	147.237.77.216	dover.idf.i		drop	drop	1422
149.88.104.157	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	235
79.183.149.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
85.250.33.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
46.19.85.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
46.116.85.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
84.108.138.140	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
176.12.146.69	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.121.253.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
176.12.147.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
79.176.60.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
220.255.1.109	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.65.58.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.246.74.109	Sweden	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	10
84.228.144.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
203.127.58.228	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
209.91.107.213	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
213.8.124.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
188.165.15.241	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
80.178.6.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
2.52.7.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
208.69.40.107	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
85.130.194.151	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	6
46.19.85.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
142.4.38.36	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
186.223.166.167	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
203.127.58.231	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.130.194.151	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
220.255.1.157	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.130.194.151	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
70.211.138.144	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
220.255.1.138	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
176.224.43.165	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5

04-11-2015-09:03:09 to 04-11-2015-10:03:09

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
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	3
24.202.72.95	Canada	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.147	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oproles/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	1
79.183.132.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
180.76.4.248	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
109.67.116.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
37.202.117.36	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/may/barg.stm	Block	1
79.183.132.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
112.111.188.90	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
216.218.206.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.114	Block	1
94.73.140.66	Turkey	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.82	Block	1
77.127.90.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0731-1.stm	Block	1
94.73.140.66	Turkey	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/093.stm	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/010.stm	Block	1
79.179.135.182	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
94.73.140.66	Turkey	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for /	Block	1

04-11-2015-09:03:09 to 04-11-2015-10:03:09