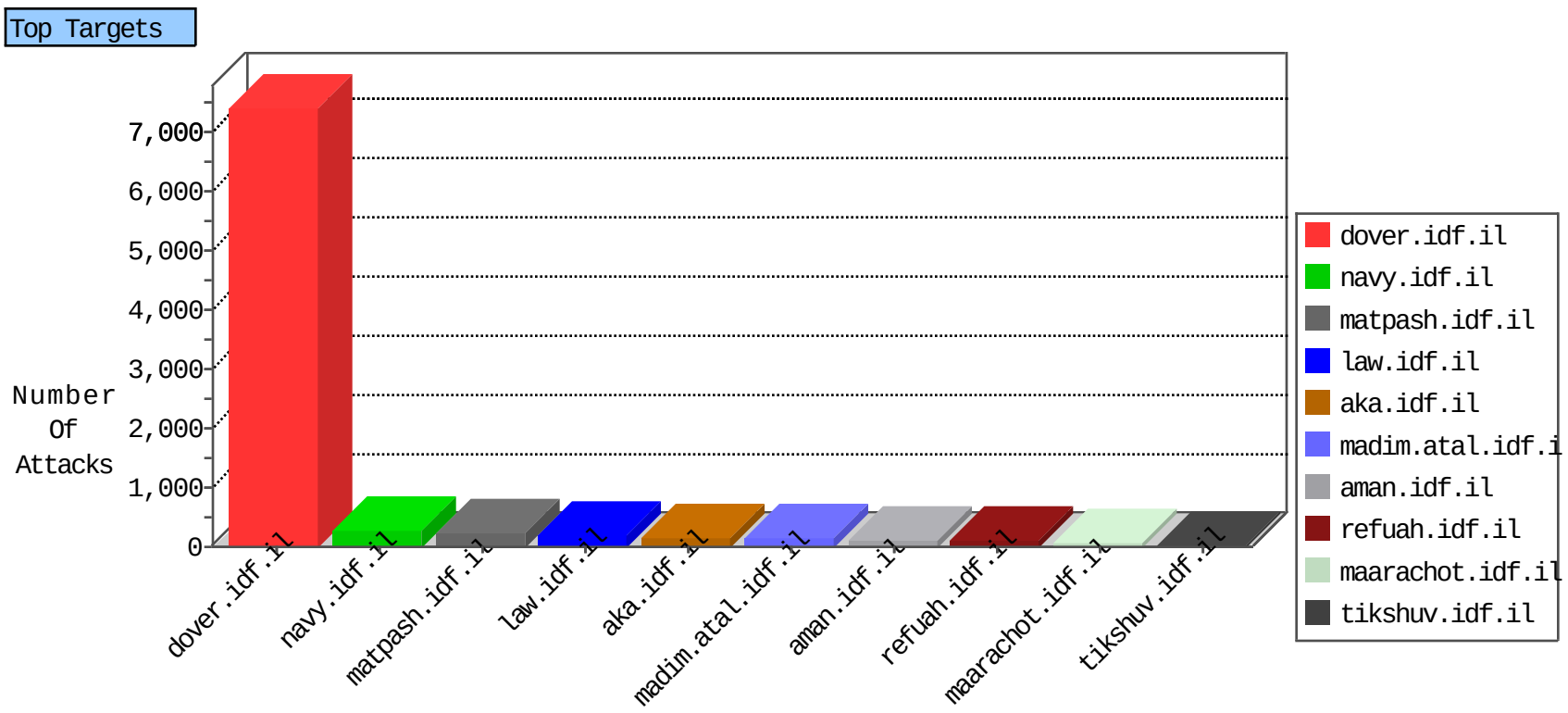
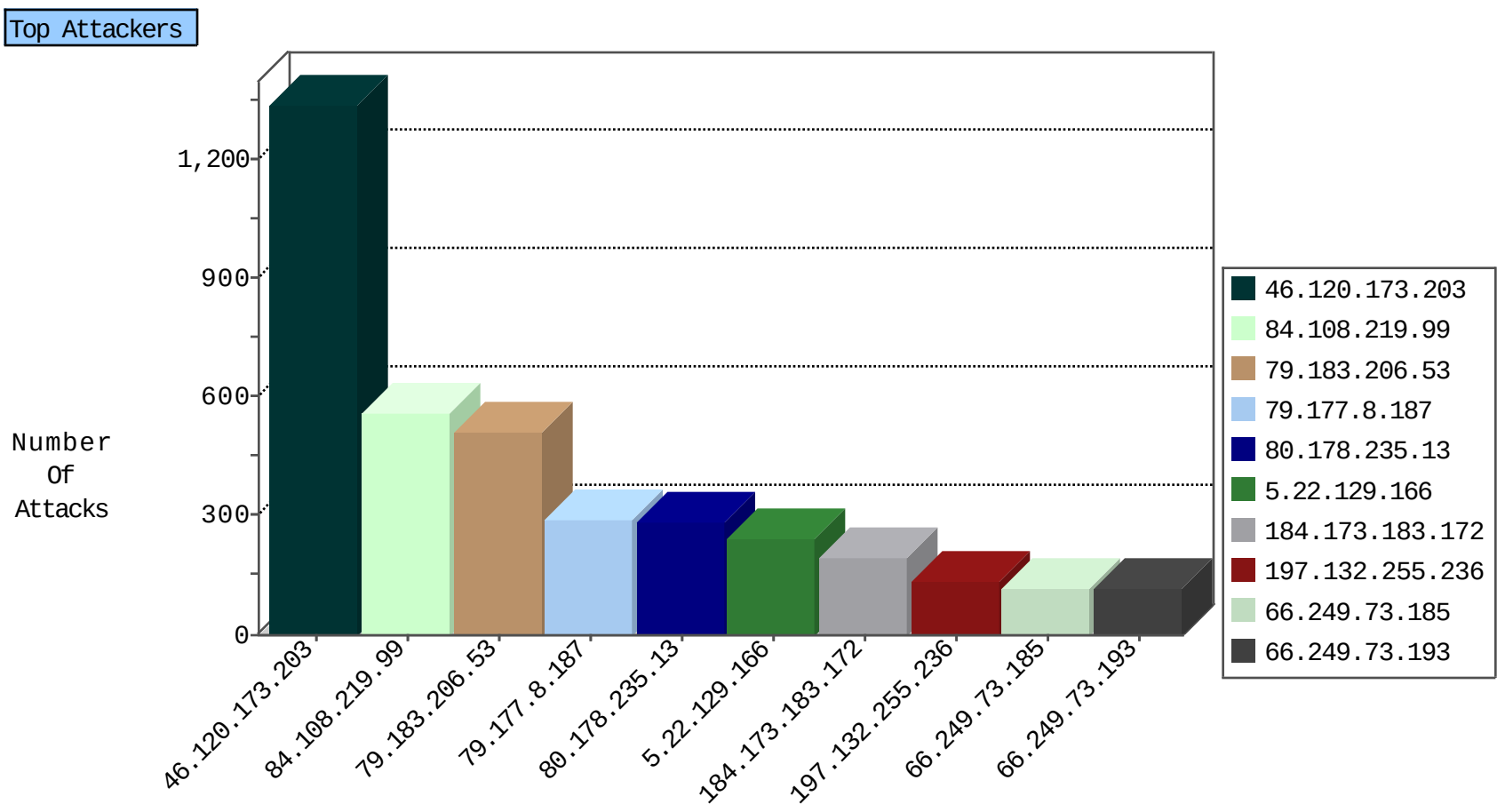
04-09-2015-18:03:03 to 04-09-2015-19:03:03

IDF Under Attack
04-09-2015-18:03:03

Top Targets



Top Attackers



04-09-2015-18:03:03 to 04-09-2015-19:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.229.185.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	389
213.57.230.59	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	255
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	116
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	116
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	106
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	70
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	63
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	60
66.249.93.135	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	52
66.249.93.254	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	41
66.249.93.131	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	34
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	27
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	27
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.78.104	United States	147.237.77.170	maarachot.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	21
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	20
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
104.35.147.135		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
77.125.252.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.81.218	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.75.111	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	15
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	12
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
23.116.35.145	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.81.212	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.73.239	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	7
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
85.64.80.33	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5

04-09-2015-18:03:03 to 04-09-2015-19:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	193
106.138.244.64	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
202.22.195.18	Bangladesh	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
105.155.127.241	Morocco	147.237.77.216	dover.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	1
128.73.208.203	Russian Federation	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
93.120.27.62	Romania	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
94.249.91.51	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-09-2015-18:03:03 to 04-09-2015-19:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
46.19.85.216	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
213.57.32.108	Israel	147.237.76.86	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
37.26.146.209	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
43.255.191.165	Japan	147.237.77.233	atal.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
43.255.191.165	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
221.231.154.22	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.7.37.194	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.76.147	chinuch.aka.idf.il	ET SCAN Rapid IMAP Connections - Possible Brute Force Attack	1
37.231.29.9	Kuwait	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.7.37.194	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
109.253.139.84	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-09-2015-18:03:03 to 04-09-2015-19:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.120.173.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1340
84.108.219.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	560
79.183.206.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	510
79.177.8.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	293
80.178.235.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	284
5.22.129.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	240
197.132.255.236	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	137
37.26.146.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
76.240.160.201	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
188.49.98.49	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
109.66.115.240	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
79.180.111.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
208.74.240.254	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
149.78.253.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
213.175.183.170	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
46.218.60.66	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
2.52.31.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
5.29.42.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
46.19.85.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
41.137.68.8	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
109.253.135.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
82.102.141.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
94.249.55.195	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
109.64.122.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
109.253.146.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
92.24.104.154	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
109.253.138.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
87.178.167.240	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
176.12.138.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
41.46.60.28	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
69.248.82.82	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
79.183.192.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
105.158.243.223	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
46.120.138.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
107.77.68.28	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
176.12.144.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
192.124.246.48	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
109.253.131.62	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
79.181.31.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
140.153.170.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
5.22.129.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
85.65.74.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
23.116.35.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.253.132.78	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
176.12.143.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.132.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	115
109.253.138.56	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.138.56	Block	23
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
109.66.174.121	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
93.172.15.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
128.73.208.203	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
142.4.38.36	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 142.4.38.36	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
41.250.30.219	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1599-14855-he/dover.aspx4	Block	2
109.160.253.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.109.149.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.125.252.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
78.174.214.107	Turkey	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
79.181.155.17	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
41.250.30.219	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.250.30.219	Block	1
84.228.111.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
79.176.122.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
213.8.129.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
54.172.196.207	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.29.42.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.109.3.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/links.stm	Block	1
85.64.56.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
79.176.122.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
217.132.126.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
54.200.99.21	United States	147.237.77.74	law.idf.il	URL is Above Root Directory www.mag.idf.il/../images/trans.gif	Block	1
142.4.38.36	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/editor/editor/	Block	1
5.29.85.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
197.246.74.15	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qar/	Block	1
128.73.208.203	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login/	Block	1
79.181.38.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
157.55.39.55	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176//	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.111.103.212	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	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
136.243.36.88	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
107.77.94.33	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forgotpassword.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefronthomefront2.stm	Block	1
109.253.138.56	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
41.238.244.196	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qar/	Block	1
84.228.71.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
207.46.13.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1415-he/dover.aspx	Block	1
79.176.122.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.220.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
142.4.38.36	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
109.64.101.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.108.123.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-09-2015-18:03:03 to 04-09-2015-19:03:03