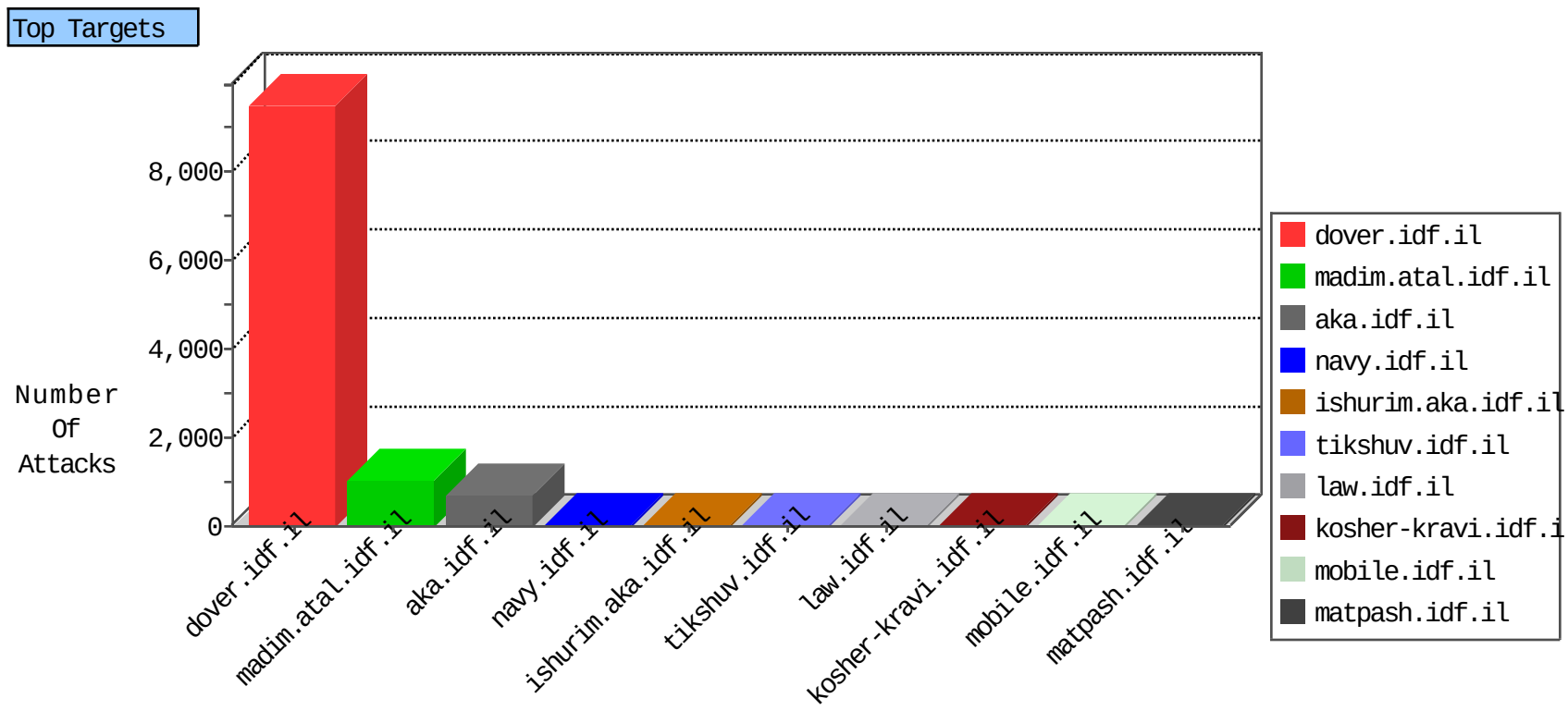
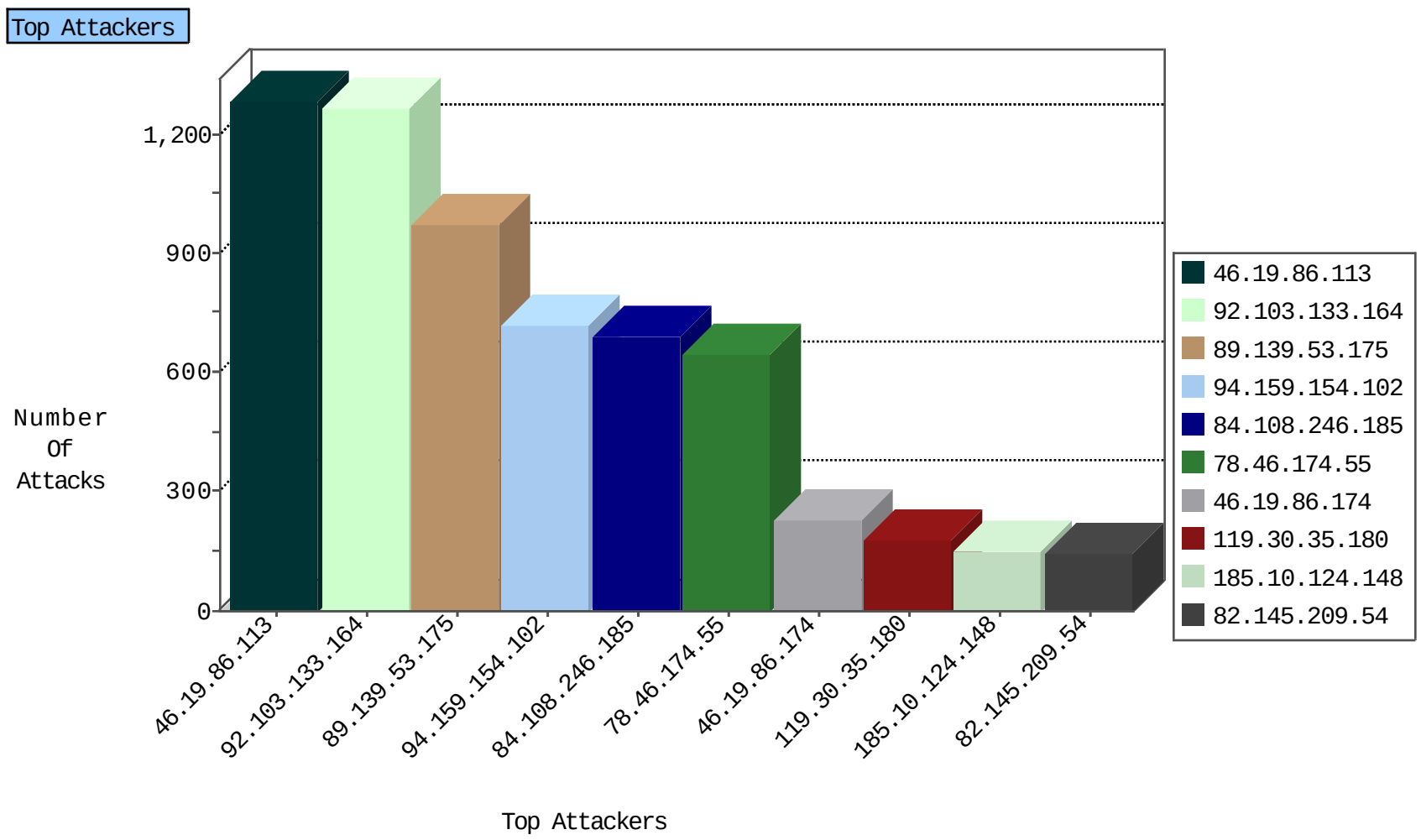
04-17-2015-18:03:01 to 04-17-2015-19:03:01

IDF Under Attack
04-17-2015-18:03:01

Top Targets



Top Attackers



04-17-2015-18:03:01 to 04-17-2015-19:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4278
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	430
84.109.210.29	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
204.93.154.199	United States	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	172
93.173.12.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
82.145.211.110	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	23
84.228.108.97	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
84.228.108.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.240.236.119	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
1.64.228.213	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
2.54.159.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-17-2015-18:03:01 to 04-17-2015-19:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	27
119.30.35.180	Bangladesh	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.51	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.116.164.9	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.250	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
213.57.254.98	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.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	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.35	akaws.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
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.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
66.240.236.119	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1

04-17-2015-18:03:01 to 04-17-2015-19:03:01

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
66.249.81.202	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
79.182.60.25	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
212.86.219.134	Germany	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
91.238.134.92	Poland	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.247.43	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -f -sS	1
199.68.196.123	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
88.249.106.23	Turkey	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1

04-17-2015-18:03:01 to 04-17-2015-19:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1283
92.103.133.164	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1264
94.159.154.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	717
84.108.246.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	689
46.19.86.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	226
185.10.124.148	Hungary	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
82.145.209.54	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	144
46.116.143.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
119.30.35.180	Bangladesh	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
37.26.148.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	115
31.168.164.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
2.54.150.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
2.54.159.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
46.19.85.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	73
5.162.202.138	Oman	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
79.182.60.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	68
2.54.23.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
72.67.166.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
84.111.80.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
213.57.242.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
213.57.136.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
46.19.86.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
128.227.41.40	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
85.65.247.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
37.26.148.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
138.162.128.54	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
84.108.170.211	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
109.253.145.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
24.189.125.63	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
46.19.86.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
93.172.45.117	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
176.12.150.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
109.253.140.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
37.142.151.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
84.228.235.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
109.253.142.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
176.12.146.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
46.19.86.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
46.19.85.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.19.86.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
46.120.194.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
81.218.143.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
176.12.150.17	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
84.111.185.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
99.198.124.106	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.53.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	971
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	439
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	72
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	71
87.69.41.39	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.41.39	Block	37
77.127.95.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
198.58.95.238	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
77.127.95.191	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
109.67.139.157	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluimtemplates/inner.asp	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
69.30.240.46	United States	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorttype in aka.idf.il/eitan/listpage/	None	1
107.170.62.85	United States	147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
84.108.220.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.148.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
62.90.235.246	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.173.162.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.58.178.57	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.218	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/sip_storage/files/5/68625	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
84.228.99.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.116.241.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.143.232.40	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.130	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/iturim/asp/results.asp	None	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
94.45.70.226	Ukraine	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/894-en/matpash.aspx	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/×ª/main/giyus	Block	1
2.54.190.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter tablequery in aka.idf.il/eitan/listpage/	None	1
162.243.251.175	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/displayallsoliders.asp	Block	1
66.249.78.6	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8745-he/navy.aspx	Block	1
87.68.157.236	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.117.16.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
193.239.220.249	Switzerland	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.130	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/results.asp	None	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
94.217.151.148	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.176.108.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.142.58.65	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
162.243.251.175	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /	Block	1

04-17-2015-18:03:01 to 04-17-2015-19:03:01