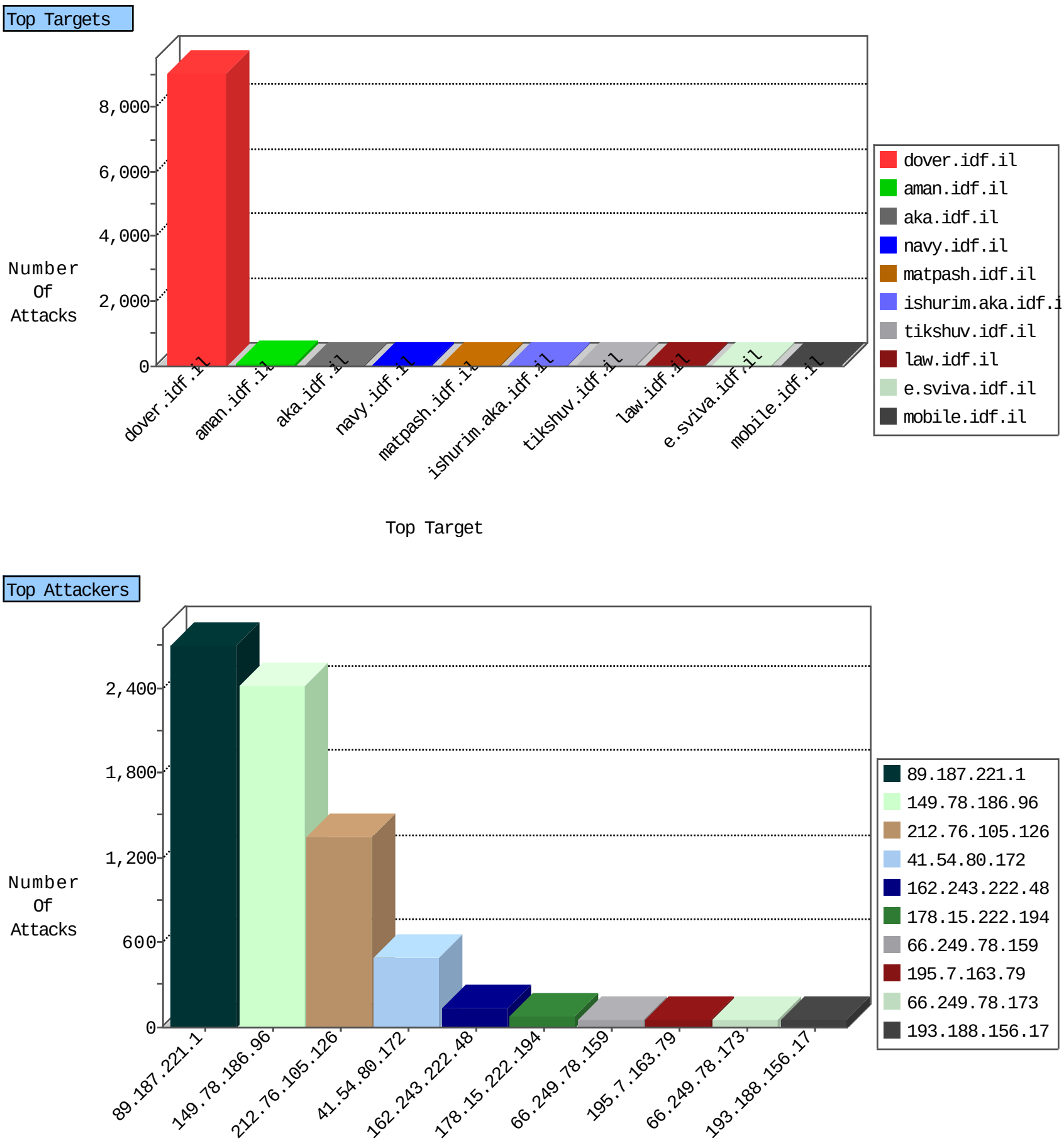
05-08-2015-13:03:01 to 05-08-2015-14:03:01

IDF Under Attack
05-08-2015-13:03:01



05-08-2015-13:03:01 to 05-08-2015-14:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6537
173.252.73.116	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4746
87.68.22.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
149.88.102.174	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
84.111.168.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
149.78.102.119	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
118.174.194.82	Thailand	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	3
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
82.166.184.140	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
75.115.46.40	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
46.183.220.250	Latvia	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
212.76.127.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
124.232.142.220	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

05-08-2015-13:03:01 to 05-08-2015-14:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
94.230.86.243	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.189	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.35	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.103.30	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
84.109.48.67	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
149.78.218.140	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
182.73.13.118	India	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.101	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	147.237.8.28	e.mobile-ks.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
198.20.70.114	United States	147.237.76.31	nakchal.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
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.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
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1

05-08-2015-13:03:01 to 05-08-2015-14:03:01

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	6
79.178.172.60	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
196.26.82.212	South Africa	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
84.94.186.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.147.96.92	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	India	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.178	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
183.247.165.129	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	ET DROP Dshield Block Listed Source	1
222.186.56.178	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
183.247.165.129	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

05-08-2015-13:03:01 to 05-08-2015-14:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2706
149.78.186.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2418
212.76.105.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1348
41.54.80.172	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	491
162.243.222.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	134
178.15.222.194	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
195.7.163.79	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
79.181.129.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
149.78.102.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
193.188.156.17	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
213.205.229.115	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
72.65.204.50	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
94.159.161.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
118.241.234.224	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
84.109.139.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
85.250.119.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
79.182.200.252	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
193.188.156.17	Sweden	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	20
80.246.133.232	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.120.196.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
87.69.81.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
93.173.182.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
84.109.138.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
185.58.14.99		147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.121.72.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
93.172.54.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
185.58.14.99		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.94.186.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
24.90.111.185	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.183.144.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.64.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	10
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	5
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	5
85.250.119.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	3
79.183.126.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.181.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.78.118	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0404-2.stm	Block	1
107.152.128.27	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-14553-en/dover.aspx/rk=0/rs=1sr66ck1mfv.f6j6ox6eiig07xo-	Block	1
66.249.64.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
37.49.97.38	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0128-3.stm	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.78.125	Block	1
207.46.13.130	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	1
109.66.81.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
79.181.235.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.67.36	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
46.120.216.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/hativa7/kkkkkkk=cd07bd0bkkkkkk_cd07bd0b	Block	1
89.139.2.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
213.8.129.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.143.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.209	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx)	Block	1
180.76.4.242	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
46.121.233.35	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
93.173.159.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.244	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/general	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.126.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
183.38.121.176	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
62.105.140.248	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan/eged.stm	Block	1
95.86.89.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.64.246	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il//giyus/forum/asp/showforum.asp	Block	1
157.55.39.151	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//library/manage/resource/getfilecontent.hh.asp	Block	1