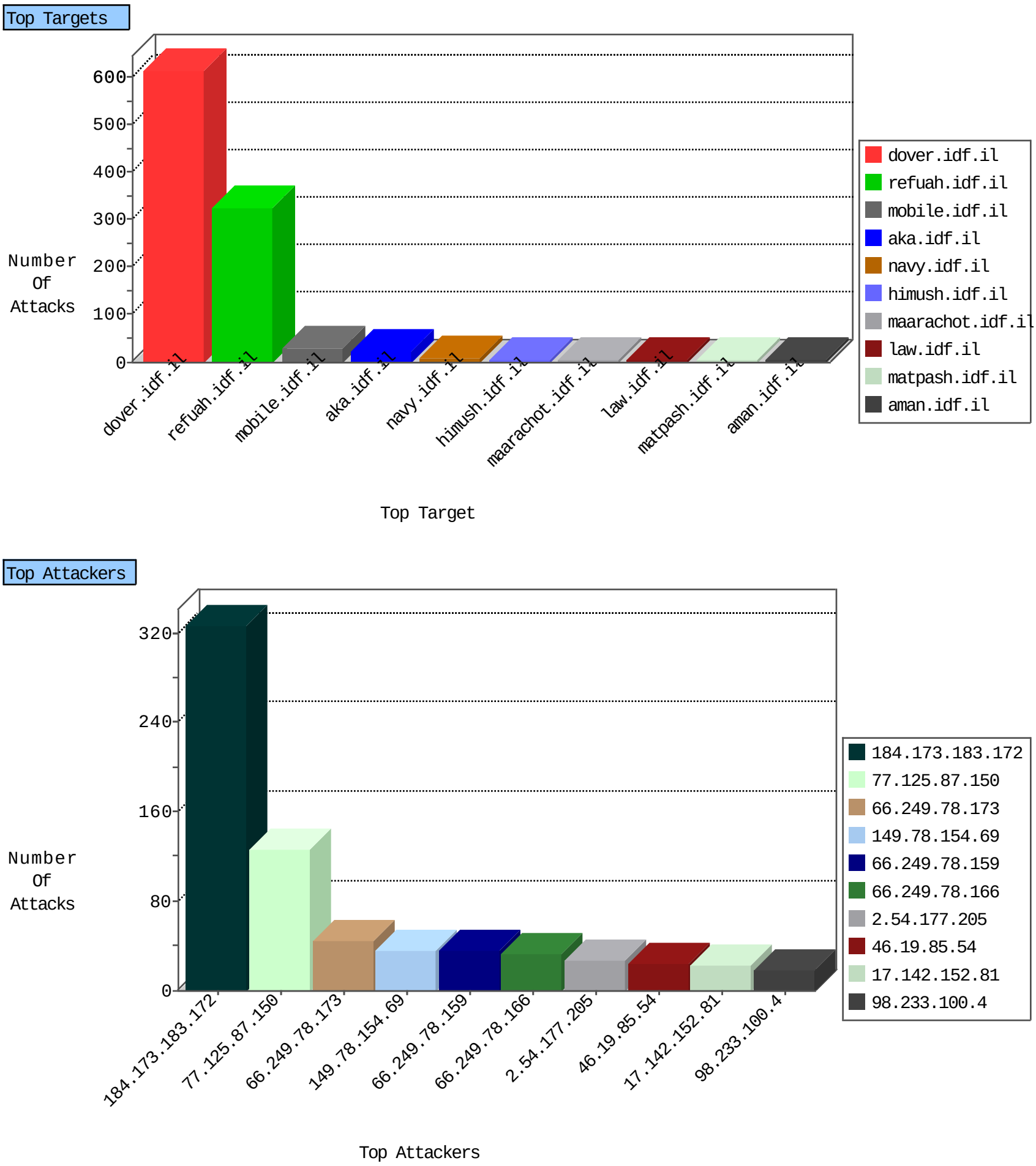
05-08-2015-04:03:05 to 05-08-2015-05:03:05

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



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
200.158.43.180	Brazil	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
171.96.187.58	Thailand	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
192.3.207.66	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	134
77.125.87.150	Israel	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	126
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
93.114.44.187	Anonymous Proxy	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
218.30.103.52	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.31	nakchal.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
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.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
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
46.249.43.105	Netherlands	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.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
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	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
109.201.154.140	Netherlands	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1

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

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	6
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
211.149.240.162	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.149.240.162	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.4	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.27	Netherlands	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
77.104.110.103	Iran, Islamic Republic of	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.240.162	China	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.149.240.162	China	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.136.216.4	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
77.104.110.103	Iran, Islamic Republic of	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 4096	1
77.104.110.103	Iran, Islamic Republic of	147.237.76.30	himush.idf.il	ET SCAN NMAP -f -sS	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
2.54.177.205	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
46.19.85.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
17.142.152.81	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
17.142.152.94	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
98.233.100.4	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
17.142.152.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
17.142.152.85	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
17.142.151.79	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
80.246.133.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
17.142.152.72	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
69.38.189.130	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
17.142.152.86	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
206.116.206.124	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.135	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
96.232.32.27	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
173.252.110.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
81.218.80.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
174.236.195.237	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
62.210.138.75	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
174.236.195.237	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
173.252.110.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
189.6.17.221	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
173.252.110.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
173.252.110.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.180.7.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
125.65.112.8	China	147.237.77.170	maarachot.idf.il	SAM rule	drop	drop	3
65.28.43.111	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.152.111	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.130.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
173.252.110.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.46.13.99	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	4
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	3
157.55.39.151	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/givati/	Block	1
119.17.49.22	Australia	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
66.249.78.134	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	1
207.46.13.13	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/925-he/atal.aspx	Block	1
46.249.43.105	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
157.55.39.137	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
69.30.240.46	United States	147.237.76.30	himush.idf.il	Illegal HTTP Version	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/writetous/default.asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17055-en/dover.aspx/trackback/	Block	1
66.249.78.141	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
71.62.3.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=3ab08fc7kkkkkkk_3ab08fc7	Block	1
157.55.39.3	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1413-he/atal.aspx	Block	1
66.249.78.148	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/haredim/maslulimlist.aspx	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74//templates/getfile/getfile.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.121.116.113	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/896-he/atal.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
207.46.13.99	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers/contact	Block	1
91.121.116.113	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/march/31.stm	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/869-4395-he/patzar.aspx	Block	1
184.105.247.196	United States	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/	Block	1

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